Quest® NetVault® Backup Plug-in *for VMware*

version 2.6

User's Guide

VMW-101-2.6-EN-01 07/29/13

QUEST SOFTWARE®
Simplicity At Work®

© 2013 Quest Software, Inc.
ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software, Inc.

The information in this document is provided in connection with Quest products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest products. **EXCEPT AS SET FORTH IN QUEST'S TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.** Quest makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software World Headquarters
LEGAL Dept
5 Polaris Way
Aliso Viejo, CA 92656
email: legal@quest.com

Refer to our Web site (www.quest.com) for regional and international office information.

Patents

This product is protected by U.S. Patents # 7,814,260; 7,913,043; 7,979,650; 8,086,782; 8,145,864; 8,171,247; 8,255,654; and 8,271,755. Protected by Japanese, E.U., French and UK patents 1615131 and 05250687.0, and German patent DE602004002858. Additional patents pending.

Trademarks

Quest, Quest Software, the Quest Software logo, Simplicity at Work, FlashRestore, GigaOS, and NetVault are trademarks and registered trademarks of Quest Software, Inc., and its subsidiaries. For a complete list of Quest Software's trademarks, please see http://www.quest.com/legal/trademarks.aspx. Other trademarks and registered trademarks are property of their respective owners.

QUEST SOFTWARE®
Simplicity At Work™

Table of Contents

Chapter 1: Introducing Quest NetVault Backup Plug-in *for VMware* 7

- **Quest NetVault Backup Plug-in *for VMware* – At a Glance 7**
- **Key Benefits 8**
- **Feature Summary 9**
- **Target Audience 9**
- **Recommended Additional Reading 10**
- **About Quest Software 10**

Chapter 2: Installing the Plug-in 13

- **Available Editions 13**
- **Deploying Plug-in *for VMware* 13**
- **Prerequisites 14**
- **Installing Plug-in *for VMware* 15**
- **Removing Plug-in *for VMware* 16**

Chapter 3: Configuring the Plug-in 17

- **Adding a Server 17**
  - *Reconfiguring an Added Server 18*
  - *Removing a Server 18*
- **Configuring Default Settings 19**
- **Enabling Virtual Machine Locking 21**
- **Additional Notes 22**
  - *Supported Backup Consistency States 22*

Chapter 4: Defining a Backup Strategy 25

- **Available Backup Methods and Backup Types 25**
  - *Image-Level Backups 25*
  - *File-Level Backups 27*
- **Defining a Backup Strategy 28**
  - *Examples 29*

Chapter 5: Performing Image-Level Backups 31

- **Performing Image-Level Backups 31**
  - *Selecting Data for a Backup 31*
  - *Setting Backup Options 36*
  - *Finalizing and Submitting a Job 41*
- **Additional Notes 42**
  - *Considerations for RDM Disks 42*
  - *Disabling CBT for a Virtual Machine 43*

Chapter 6: Performing File-Level Backups 45

- **Performing File-Level Backups 45**
  - *Selecting Data for a Backup 45*
  - *Setting Backup Options 48*
  - *Finalizing and Submitting a Job 50*
- **Additional Notes 51**
  - *Manually Removing the Snapshot and Mount Folder 51*

Chapter 7: Restoring Image-Level Backups 53

- **Available Restore Types for Image-Level Backups 54**
- **Recovering a Full Virtual Machine from Image-Level Backups 55**
  - *Prerequisites 55*
  - *Selecting Data for a Restore 55*
  - *Setting Restore Options 56*
  - *Finalizing and Submitting a Job 58*
  - *Starting the Virtual Machine 59*
- **Advanced Restore Procedures 59**
  - *Relocating a Virtual Machine to an Alternate ESX Server Host 59*
  - *Renaming a Virtual Machine During Restore 59*
- **Performing File-Level Restores from Image-Level Backups 60**
  - *Selecting Data for a Restore 60*
  - *Setting Restore Options 62*
  - *Finalizing and Submitting a Job 63*
- **Restoring Virtual Machine Disk and Configuration Files 63**
  - *Selecting Data for a Restore 63*
  - *Setting Restore Options 64*
  - *Finalizing and Submitting a Job 65*
  - *Recovering a Virtual Machine From the Restored Files 65*
- **Additional Features Available on the Selections Tab 66**

Chapter 8: Restoring File-Level Backups 69

- **Available Restore Methods for File-Level Backups 69**
- **Restoring File-Level Backups Using Shared Network Drives 70**
  - *Setting Up a Network Share 70*
  - *Selecting Data for a Restore 70*
  - *Setting Restore Options 71*
  - *Finalizing and Submitting a Job 72*
- **Restoring File-Level Backups Using the Native Plug-in for FileSystem 73**
  - *Prerequisites 73*
  - *Restoring Data 73*
- **Additional Features Available on the Selections Tab 74**

Chapter 9: Troubleshooting 77

- **Common Errors 77**
- **SOAP Messages 80**
- **VDDK Logs 80**

Chapter 1:

INTRODUCING QUEST NETVAULT BACKUP PLUG-IN *FOR VMWARE*

- Quest NetVault Backup Plug-in for VMware – At a Glance
- Key Benefits
- Feature Summary
- Target Audience
- Recommended Additional Reading
- About Quest Software

1.1.0 Quest NetVault Backup Plug-in *for VMware* – At a Glance

Quest NetVault Backup Plug-in *for VMware* (Plug-in *for VMware*) eliminates the need for complex scripting and does not require that you understand ESX or vStorage APIs for Data Protection (VADP) internals to protect your VMware environment and achieve faster and more reliable recoveries. It protects virtual machines from disasters, media failure, and data corruption. An intuitive, easy-to-use GUI gives you a single, centralized console to configure backup and restore policies for your virtual environments. The plug-in offers granular control that minimizes downtime by allowing you to restore complete virtual machine images or individual files quickly and reliably with minimal interaction. Through automatic integration with a wide range of backup devices, your virtualized data can be protected and safely stored offsite to meet your disaster recovery and business continuity goals.

Note: Quest NetVault Backup Plug-ins for applications such as Exchange, SQL Server, or SharePoint can be combined with the Plug-in *for VMware* to provide comprehensive protection to your data. The Plug-in *for VMware* provides virtual machine bare metal recovery, while the application plug-ins simplify data protection of business-critical applications by automating the backup and recovery processes and performing important maintenance functions, such as transaction log truncation.

1.2.0 Key Benefits

- **Improve VMware ESX Performance With VADP** – The Plug-in *for VMware* works with VADP to provide centralized backups that reduce the load on each VMware ESX Server, allowing them to run more virtual machines and reduce backup traffic on the Local Area Network. This approach is especially important if you need to consolidate hardware. You have the flexibility to protect all your virtual machines deployed on a single VMware ESX Server or protect multiple VMware ESX Servers from a single Quest NetVault Backup (NetVault Backup or NVBU) Client. The Plug-in *for VMware* benefits from VMotion's ability to track the deployment of virtual machines to ensure that backups and restores are performed without requiring detailed knowledge of the location of the individual virtual machines.
- **Increase Confidence while Deploying VMware** – The Plug-in *for VMware* protects an individual ESX Server or a full vCenter environment while empowering you to create comprehensive, flexible backup policies without the need to understand VADP internals or create complex scripting. The plug-in provides peace of mind because users can simply point-and-click to back up or restore virtual machines. It increases efficiency by consolidating virtual machine backup management into the NVBU environment. Additionally, the plug-in enhances Windows protection by performing VSS-based snapshots to quiesce VSS-enabled applications before a backup.
- **Automatic Integration of Backup Devices Ensures Business Continuity** – With offsite backups being an important part of the data protection plan for any mission critical application, the Plug-in *for VMware* takes advantage of NVBU's fundamental integration with a wide range of backup devices. The Plug-in *for VMware* ensures that your virtualized environments are protected and stored offsite for disaster recovery purposes. It also frees administrators from being available 24x7 by allowing less experienced VMware administrators to confidently initiate restores correctly and as quickly as possible, reducing downtime and improving business continuity.
- **Shorten Backup Windows and Improve Device Utilization** – The Plug-in *for VMware* speeds virtual machine image-based backups with high performance Incremental and Differential Backups for data stored in virtual machines. The plug-in integrates with VMware's Changed Block Tracking (CBT) to ensure that only blocks that have changed since the initial Full, and the last Incremental or Differential Backup are sent to the current Incremental or Differential backup stream to give you more efficient backups and reduced network demands.

The Plug-in *for VMware* also preserves the use of VMware's Thin Disk Provisioning feature during virtual machine recovery operations to control storage costs and protect data by ensuring virtual machine disks only use the amount of storage they currently need while being able to dynamically add more allocated space as required.

1.3.0 Feature Summary

- Supports VADP-based online backups
- Creates VSS-based snapshots for application-consistent backups
- Integrates with VADP and CBT
- Supports backup and restore of VMware Thin Provisioned Disks
- Enables backup and restore of virtual machines within a Virtual Application (vApp)
- Supports VMotion using new vSphere virtual machine locking API
- Allows Full, Incremental, and Differential image-level backups of virtual machines
- Reduces backup windows by backing up multiple virtual machines in parallel
- Reduces network and storage requirements for NTFS basic disks with Active Block Mapping (ABM)
- Allows Full, Differential, and Incremental file-level backups of Windows Guest OS
- Offers ease of use with point-and-click GUI
- Restores complete virtual machine image or individual files
- Relocates virtual machines to alternate ESX Server host
- Renames virtual machines during restore
- Allows file-level restores from image-level backups
- Relocates individual files to alternate directory or virtual machine

1.4.0 Target Audience

This guide is intended for users who are responsible for the backup and recovery of VMware virtual machines. Familiarity with vCenter/ESX Server administration and the operating system under which the virtual machines are running is assumed. Advanced knowledge of VMware would be useful for defining an efficient backup and recovery strategy for the virtual machines.

1.5.0 Recommended Additional Reading

- **NetVault Backup Documentation**

  You can download the complete set of NetVault Backup documentation from the Quest Software web site at the following address:

  https://support.quest.com/Search/SearchDownloads.aspx

- **VMware Documentation**

  You can download the complete set of VMware documentation at:

  http://www.vmware.com/support/pubs

1.6.0 About Quest Software

Established in 1987, Quest Software **(Nasdaq: QSFT)** provides simple and innovative IT management solutions that enable more than 100,000 global customers to save time and money across physical and virtual environments. Quest products solve complex IT challenges ranging from database management, data protection, identity and access management, monitoring, user workspace management to Windows management. For more information, visit www.quest.com.

Contacting Quest Software

Email:	info@quest.com
Mail:	Quest Software, Inc. World Headquarters 5 Polaris Way Aliso Viejo, CA 92656 USA
Web site:	www.quest.com

For regional and international office information, refer to the web site.

Quest Support

Quest Support is available to customers who have a trial version of a Quest product or who have purchased a Quest product and have a valid maintenance contract. Quest Support provides unlimited 24x7 access to our Support Portal at www.quest.com/support.

From our Support Portal, you can do the following:

- Retrieve thousands of solutions from our Knowledge Base
- Download the latest releases and service packs
- Create, update, and review Support cases

View the *Global Support Guide* for a detailed explanation of support programs, online services, contact information, policies and procedures.

The guide is available at www.quest.com/support.

This guide is available in English only.

Chapter 2:

INSTALLING THE PLUG-IN

- Available Editions
- Deploying Plug-in for VMware
- Prerequisites
- Installing Plug-in for VMware
- Removing Plug-in for VMware

2.1.0 Available Editions

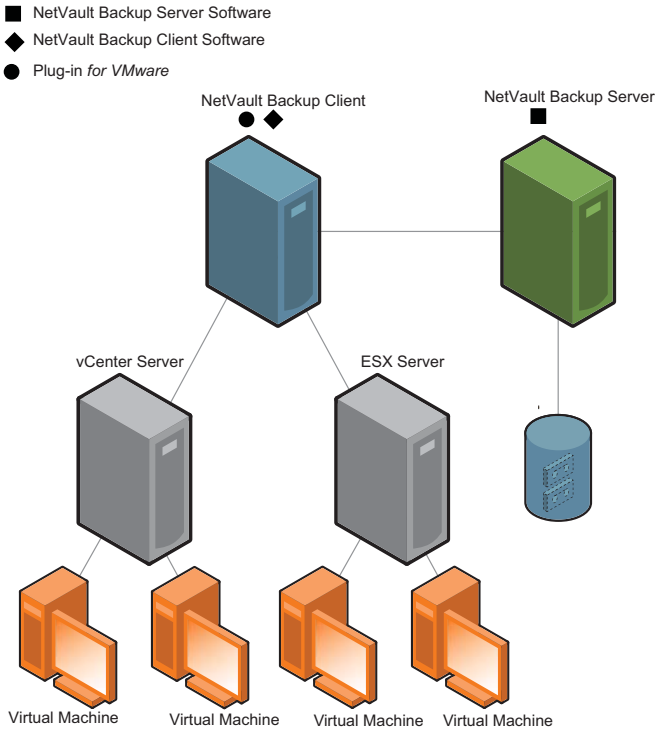
The Plug-in *for VMware* is available in two editions.

- **ESX Server Edition** – The ESX Server Edition provides protection to virtual machines hosted by one or more ESX Servers. This edition can be deployed on any Windows-based or Linux-based NVBU Client. The number of ESX Servers that you can add to a client running the ESX Server Edition of the plug-in will depend on the capacity specified in the purchased license.
- **Enterprise Edition** – The Enterprise Edition provides protection to virtual machines controlled by one or more ESX or vCenter Servers. This edition can be deployed on any Windows-based or Linux-based NVBU Client. You can add any number of ESX or vCenter Servers to a client running the Enterprise Edition of the plug-in.

2.2.0 Deploying Plug-in *for VMware*

The Plug-in *for VMware* can be deployed on any Windows-based or Linux-based NVBU Client that has access to the virtual disk storage. This type of deployment enables centralized backup administration and off loads backup I/O from the ESX Server. The ESX Server is only required to generate the snapshot checkpoint which is recorded in the disk. This results in a minimal performance impact on the ESX Server. With a vCenter Server, the plug-in takes advantage of the vMotion technology to track migration and automatically back up a virtual machine from its current host.

Figure 2-1: *Plug-in for VMware Deployment*



2.3.0 Prerequisites

Before you start the installation procedure, make sure that the following requirements are met:

- **Install the NVBU Client Software** – Install the NVBU Client software on the system that will host the Plug-in *for VMware*. For LAN-free backups, you require an NVBU SmartClient license. For more information about installing the NVBU Client software, refer to the *Quest NetVault Backup Installation Guide*.

Note: The Linux version of the Plug-in *for VMware* does not support file-level backups of virtual machines. To perform file-level backups, you must install the plug-in on a Windows-based NVBU Client.

- **Virtual Disk Storage Requirements**
  - The virtual machines that you want to back up must use virtual disks that reside on VMFS datastores created on local storage, iSCSI, or FC SAN. The plug-in also supports virtual machines that use Raw Device Mapping (RDM) disks in virtual compatibility mode.

- To use LAN Transport Mode, the virtual disk files should not exceed 1TB in size.
- With FC SAN storage, you require a dedicated physical machine to host the plug-in.

  With iSCSI storage and any type of storage that supports the NBD format including ESX Server's local storage, a physical machine is not required. You can configure one of the virtual machines as an NVBU Client to host the plug-in.
- With SAN storage, the NVBU Client requires read/write access to the SAN LUNs which contain the VMFS volumes (datastores) with virtual disks or the virtual compatibility RDMs. To ensure this, add the NVBU Client to the same fabric zones to which the ESX Server system belongs.

  Additionally, configure the same host mode (connection type) settings on the NVBU Client and the ESX Server. For example, if you have an IBM array and the host mode setting is LNXCL, set the same for the NVBU Client.

- **Enable SSL Certificate Verification** – When communicating with the vCenter or ESX Server, the Plug-in *for VMware* can transfer data over an encrypted SSL connection or an unencrypted network channel.

  You can use an unencrypted channel if there is a trusted environment with fully isolated transmissions between the ESX Server and NVBU Client. Disabling SSL can improve performance because you avoid the overhead required to perform encryption.

  To secure the communication channel, enable SSL certificate verification in your virtual environment. It is not enabled by default.
- **Add the NVBU Client** – Add the designated NVBU Client to the NVBU Server. For more information about adding NVBU Clients, refer to the *Quest NetVault Backup Administrator's Guide*.

2.4.0 Installing Plug-in *for VMware*

To install the Plug-in *for VMware*, follow these steps:

1. Start the NVBU Console on the NVBU Server, and open the **NVBU Client Management** window. To open this window:
   - Click **Client Management** on the toolbar or **Large Buttons** panel.
   - Alternatively, on the **Administration** menu, click **Client Management**.
2. In the **Clients** list, right-click the NVBU Client on which you want to install the plug-in, and select **Install Software**.

3. In the browse window, navigate to the location of the **.npk** installation file for Plug-in *for VMware* (on the installation CD or the directory to which the file was downloaded from Quest Software's web site). Depending on the operating system, the file path for this software may vary on the installation CD.
4. Select the file named **vmw-x-x-x-x.npk** (where **x-x-x-x** represents the version and build numbers), and click **Open** to begin the installation process. When the installation completes, a message is displayed. Click **OK** to close the dialog.

2.5.0 Removing Plug-in *for VMware*

To remove the Plug-in *for VMware*, follow these steps:

1. Start the NVBU Console on the NVBU Server, and open the **NVBU Client Management** window.
2. In the **Clients** list, right-click the NVBU Client from which you want to remove the plug-in, and select **Remove Software**.
3. In the list of plug-ins, select **VMware Plugin**, and click **Remove**.
4. In the confirmation dialog, click **OK**.

Chapter 3:

CONFIGURING THE PLUG-IN

- Adding a Server
  - Reconfiguring an Added Server
  - Removing a Server
- Configuring Default Settings
- Enabling Virtual Machine Locking
- Additional Notes
  - Supported Backup Consistency States

3.1.0 Adding a Server

Before you can start using the plug-in for backups and restores, you must add the applicable ESX or vCenter Server to the plug-in, and configure a user account to log on to the server.

- **Standalone ESX/ESXi Server Setup** – In a VMware environment consisting of one or more ESX/ESXi Servers, you must add the individual hosts to the plug-in, and configure a user account for each server.
- **Cluster Setup** – In a cluster setup managed by a vCenter Server, you must add the vCenter Server to the plug-in, and configure account for the server.

Note: The Plug-in *for VMware* supports ESXi Servers that are in Lockdown Mode when the hosts are managed by a vCenter Server.

To add a vCenter Server or an ESX Server, follow these steps:

1. Start the NVBU Console on the NVBU Server, and open the **NVBU Backup** window. To open this window:
   - Click **Backup** on the toolbar or **Large Buttons** panel.
   - Alternatively, on the **Operations** menu, click **Backup**.
2. On the **Selections** tab, double-click the NVBU Client on which the plug-in is installed. Alternatively, right-click the client, and select **Open**.
3. In the list of plug-ins, right-click **VMware Plugin**, and select **Add Server**.
4. Configure the following parameters:

- **Server Name** – Enter the name of the ESX/ESXi Server (in a standalone server setup) or the vCenter Server (in a cluster setup). The server name must be unique. If you do not specify a name, the plug-in will assign the **Server Address** of the ESX or vCenter Server as the server name.

  You cannot change the server name once it is configured.
- **Server Address** – Enter the Fully Qualified Domain Name (FQDN) for the ESX/ESXi Server (in a standalone server setup) or the vCenter Server (in a cluster setup). You can also specify the IP address of the server, but using the FQDN is the preferred method.
- **User** – Enter a user account that can be used to log on to the vCenter or ESX Server. The user account must have permissions to register or create virtual machines.
- **Password** – Enter the password for the user account.

5. Click **OK** to close the window. The plug-in will try to log on to the server, and if successful, add the server to the backup selections tree.

3.1.1 Reconfiguring an Added Server

To change the IP address or user account for a server, follow these steps:

1. Open the **NVBU Backup** window on the NVBU Server.
2. On the **Selections** tab, double-click the NVBU Client on which the plug-in is installed. Alternatively, right-click the client, and select **Open**.
3. In the list of plug-ins, open **VMware Plugin**.
4. Right-click the server, and select **Edit Server**.
5. Reconfigure the required parameters:
   - **Server Name** – This parameter displays the server name. It is a read-only parameter.
   - **Server Address** – Enter the new FQDN for the ESX or the vCenter Server. You can also specify the IP address of the server, but using the FQDN is the preferred method.
   - **User** – Enter a new user account. The user account must have permissions to register or create virtual machines.
   - **Password** – Enter the password for the new user account.
6. Click **OK** to save the new settings.

3.1.2 Removing a Server

To remove an ESX or a vCenter Server, follow these steps:

1. Open the **NVBU Backup** window on the NVBU Server.
2. On the **Selections** tab, double-click the NVBU Client on which the plug-in is installed. Alternatively, right-click this node, and select **Open**.

3. In the list of plug-ins, open **VMware Plugin**.
4. Right-click the applicable server, and select **Remove Server**.
5. In the confirmation dialog, click **Yes**.

3.2.0 Configuring Default Settings

To configure the default settings for the Plug-in *for VMware*, follow these steps:

1. Open the plug-in configuration window.
   a. **Using NVBU Configurator**
      1.Start the NVBU Configurator.
      2.Click the **Plugin Options** tab, and then click the **VMware Plugin** subtab.
   b. **Using Remote Configurator**
      1.Open the **NVBU Client Management** window.
      2.In the **Clients** list, right-click the NVBU Server, and select **Configure**.
      3.In the **Remote Configurator** window, click the **Plugin Options** tab, and then click the **VMware Plugin** subtab.
   c. **Using NVBU Console**
      1.Open the **NVBU Backup** window.
      2.On the **Selections** tab, open the NVBU Server node.
      3.Right-click **VMware Plugin**, and select **Configure**.
2. Configure the following parameters:
   - **Transport Mode** – The supported methods for accessing the virtual machine disks include the following:
     - **SAN Mode** – The SAN transport mode can be used when the ESX/ESXi Server uses Fibre Channel or iSCSI SAN to store the virtual machine disks. The SAN mode allows you to completely off load backups to a physical NVBU Client.

       To use this transport mode, select **san** in the **Transport Mode** list. On new plug-in installations, the **san** transport mode is selected by default.

Important: To use the SAN transport mode, the NVBU Client on which the plug-in is installed must have SAN connectivity to the VMFS LUN.

     - **SCSI Hot-Add Mode** – The SCSI Hot-Add transport mode can be used when the NVBU Client is installed on a virtual machine. The SCSI Hot-Add mode eliminates the need for a dedicated physical NVBU Client and does not require you to expose SAN LUNs to the NVBU Client. It can be used with any type of storage.

This transport mode is not as efficient as the SAN mode which does not cause any overhead on the ESX Server host. However, it is more efficient than the LAN mode.

To use this transport mode, select **hotadd** in the **Transport Mode** list.

- **LAN Mode** – The LAN transport mode can be used when the ESX/ESXi Server uses local storage devices or NAS to store its virtual machine disks. In this mode, the Plug-in *for VMware* uses the Network Block Device (NBD) protocol to access virtual disks. The ESX Server host reads the data from the storage device and sends it across a network channel to the plug-in.

  The LAN transport mode does not support virtual disks that are larger than 1TB in size.

  This transport mode does not completely off load backup processes from the ESX Server. However, it supports any storage device and does not require a dedicated physical NVBU Client.

  To use the LAN transport mode, configure the parameter as follows:

  - If your ESX/ESXi Server Host and the Plug-in *for VMware* are on a secure isolated network, select **nbd** for unencrypted data transfers. This mode is faster than **nbdssl** and takes fewer resources of the ESX Server and NVBU Client.
  - To protect sensitive information using encrypted data transfers, enter **nbdssl**.

- **Fallback Transport Mode** – If your setup includes a combination of SAN, NAS, or locally-attached SCSI storage for virtual machines, you can configure a fallback transportation mode which can be used when the primary transportation mode fails.

  Depending on the type of storage your ESX/ESXi Server has access to, select **san**, **hotadd**, **nbd** or **nbdssl** in the **Fallback Transport Mode** list. If no alternative is available, select **none**. On new plug-in installations, the fallback transport mode is set to **nbd** by default.

- **Default Inventory View** – The Plug-in *for VMware* provides two View Types to browse the VMware inventory objects in the **NVBU Backup** window:

  - **Hosts and Clusters** – The **Hosts and Clusters** view provides a hierarchical view of the hosts, clusters, and their child objects. In a cluster setup (managed by a vCenter Server), this view displays the virtual machines under the Cluster node, while in a standalone ESX Server setup, it displays the virtual machines under the individual hosts. This is the default inventory view for the Plug-in *for VMware*.

    The **Hosts and Clusters** view does not include the folders created on the vCenter Server in the hierarchy.

- **VMs and Templates** – The VMs and Templates view provides a flat view of all virtual machines and templates in the inventory, grouped by the datacenters and folders.

Note: To switch between the two views, right-click the server node in the **NVBU Backup** window, and select **Toggle Inventory View**. This command is only available when server node is open.

- **Progress Statistics Update Interval** – This parameter determines the interval at which the plug-in updates the progress statistics displayed in the **Job Monitor** window. By default, this window is updated every 10 seconds. To change the default interval for progress updates, enter or select the new value. The progress interval is specified in number of seconds.

Note: Frequent progress updates can have a negative impact on the performance of the plug-in.

- **Working Directory** – The Working Directory is used for the following purposes:
  - To mount virtual machine volumes during the file-level browse and backup operations.
  - To store data while restoring legacy backup savesets created with Plug-in *for VMware* v1.x.

  The default location for the Working Directory is **<NVBU Installation Directory>/tmp**. To change the location, enter the full path in **Working Directory**. Ensure that the path is valid and the configured directory already exists on the system. The Plug-in *for VMware* will not perform any path validation checks when you save the settings.

3. Click **OK** to save the settings.

3.3.0 Enabling Virtual Machine Locking

If a virtual machine is migrated (for example, through Storage vMotion) while a backup or restore job is in progress, it can cause a job to fail or create orphaned virtual disks on the datastores. To temporarily disable migration for a virtual machine when a job is in progress, the plug-in can lock the virtual machine before a job starts. When the plug-in finishes accessing the virtual disks, it unlocks the virtual machine and makes it available for migration.

By default, the locking mechanism is disabled and not used during backups and restores. To enable virtual machine locking, use the following steps:

1. Open the **vmware.cfg** file in any text editor. This file is located in the **<NVBU Installation Directory>/config** directory.

2. In the **[Custom:GetMigrationLock]** section, set the **Value** parameter to **True**:

```
[Custom:GetMigrationLock]
Value = True
```

3.4.0 Additional Notes

3.4.1 Supported Backup Consistency States

The Plug-in *for VMware* supports the following consistency states for a snapshot.

Crash-Consistent Snapshots

Crash-consistent snapshots capture the volume state as it would be after a power outage. Such snapshots are not guaranteed to be free of incomplete I/O operations or data corruption. During a restore, there can be some data loss or corruption that can cause application failure.

On non-Windows Guest OS, the Plug-in *for VMware* only supports crash-consistent snapshots.

File-System-Consistent Snapshots

For file-system-consistent snapshots, all file system I/O is temporarily frozen and dirty memory data is flushed to the disk before the snapshot is taken. This consistency state is only supported on Windows Guest OS.

Requirements for File-System-Consistent Snapshots

Guest OS Version	ESX Server Version	Requirements
Any supported Windows Guest OS	ESX Server 3.5 U2 and later	Install VSS components on the virtual machine as part of updated VMware Tools
Any supported Windows Guest OS	ESX Server prior to 3.5 U2	Install the SYNC driver included in the VMware Tools on the virtual machine.

Note: Creating quiesced snapshots using the SYNC driver requires waiting for I/O to drain in the Guest OS. This can affect time-sensitive applications.

VSS-Based Application-Consistent Snapshots

When backing up a Windows Guest OS, the Plug-in *for VMware* uses VSS to perform application-level quiescing before generating a snapshot. The application-consistent snapshots reduce the amount of application crash recovery that needs to be performed for VSS-enabled applications, like SQL Server, Exchange, and SharePoint, after restoring an image-level backup.

This consistency state is only supported on Windows 2003 and 2008.

Requirements for VSS-Based Application-Consistent Snapshots

Guest OS Version	ESX Server/ vSphere Version	Requirements
Windows 2008 Windows 2008 R2	vSphere 4.1 and later	■ Install VSS components on the virtual machine as part of updated VMware Tools. ■ Enable the UUID attribute for the virtual machine. It is enabled by default for virtual machines created on ESX 4.1 and later. To enable this attribute, see *Enabling UUID Attribute for a Windows 2008 Virtual Machine*: ■ Ensure that the virtual machines use SCSI disks only and have enough free SCSI slots as the number of disks. Application-consistent snapshots are not supported for virtual machines using IDE disks. ■ Ensure that the virtual machines do not use dynamic disks.
Windows 2003	ESX Server 3.5 U2 and later	■ Install VSS components on the virtual machine as part of updated VMware Tools.

Enabling UUID Attribute for a Windows 2008 Virtual Machine

To enable the UUID attribute for application-consistent snapshots on a Windows 2008 virtual machine, complete the following steps:

1. Start the vSphere Client.
2. Log on to the vCenter Server, and select **VMs and Templates**.
3. Click the **Virtual Machines** tab.
4. Power off the virtual machine (right-click the virtual machine, and select **Power -> Power Off**).
5. Right-click the virtual machine, and select **Edit Settings**.
6. Click the **Options** tab. In the settings column, select **General**, and then click **Configuration Parameters**.
7. In the window that appears, click **Add Row**, and configure the following parameters:
   - **Name** – Enter **disk.EnableUUID**.
   - **Value** – Enter **TRUE**.

   Click **OK**.
8. Save the settings and power on the virtual machine.

Chapter 4:

DEFINING A BACKUP STRATEGY

- Available Backup Methods and Backup Types
  - Image-Level Backups
    - Available CBT-Based Backup Types
    - Available Non-CBT Backup Types
  - File-Level Backups
    - Available File-Level Backup Types
- Defining a Backup Strategy
  - Examples

4.1.0 Available Backup Methods and Backup Types

The Plug-in *for VMware* supports both image-level and file-level backups of virtual machines. Image-level backups are operating system neutral and can be performed for any valid virtual machine; file-level backups are only supported for Windows Guest OS.

4.1.1 Image-Level Backups

An Image-Level Backup provides a point-in-time image of a virtual machine using VMware's snapshot technology. This backup can be used to perform the following types of recoveries:

- Recover a full virtual machine to a previous known state.
- Restore one or more files to a specified location.
- Restore virtual machine disk and configuration files to a specified location.

Virtual machines hosted on ESX/ESXi 4.0 and later support a feature called **Changed Block Tracking (CBT)**. CBT allows virtual machines to keep track of the changed disk sectors. When you enable this feature, a **"Change ID"** is assigned to each disk when a snapshot is generated. The Change ID identifies the state of a virtual disk at a specific point in time. The subsequent snapshots capture only the blocks that have changed since the last snapshot.

CBT offers the following advantages:

- Allows Incremental and Differential image-level backups of virtual machines.
- Often reduces the backup size of Full image-level backups because only the used sectors of a virtual disk are backed up.

CBT requires virtual hardware version 7 or later. It does not support the following disk types:

- Physical compatibility RDM virtual disks.
- Virtual compatibility RDM (Independent Disks).
- Virtual disks attached to a shared virtual SCSI bus.

4.1.1.a Available CBT-Based Backup Types

The Plug-in *for VMware* supports the following types of image-level backups for CBT-enabled virtual machines:

- **Full Backup** – A Full Backup backs up all allocated sectors on a virtual disk. Full Backups take longer to complete and consume more backup media. These backups serve as the baseline backup for future Incremental and Differential image-level backups.
- **Differential Backup** – A Differential Backup backs up disk sectors that have changed since the last Full Backup. Differential Backups speed up recovery since the plug-in is only required to restore two savesets.
- **Incremental Backup** – An Incremental Backup backs up disk sectors that have changed since the last Full, Differential, or Incremental Backup. Incremental Backups consume minimum storage space and are quicker to perform. However, data recovery takes longer and may require the plug-in to access several savesets depending on the number of incremental savesets that need to be restored.

Data Backed Up and Restored for Different Disk Types

The Plug-in *for VMware* includes the following data in a CBT-enabled backup and restore:

Disk Type	CBT-enabled Full Image Backups	Incremental/ Differential Image Backups	Restore of CBT-enabled Full Image Backups	Restore of Incremental/ Differential Image Backups
Thin (Required space supplied and zeroed out on demand.)	Only used disk sectors are backed up.	Only changed disk sectors are backed up.	Only used sectors are restored.	Only used disk sectors are restored. Each sector is restored only once.

Disk Type	CBT-enabled Full Image Backups	Incremental/ Differential Image Backups	Restore of CBT-enabled Full Image Backups	Restore of Incremental/ Differential Image Backups
Zeroed Thick (All space allocated at creation time, unused part zeroed out on first write.)	Only used disk sectors backed up.	Only changed disk sectors are backed up.	Only used sectors are restored.	Only used disk sectors are restored. Each sector is restored only once.
Eager Zeroed Thick (All space allocated and zeroed out at creation time.)	All disk sectors are backed up.	Only changed disk sectors are backed up.	The entire disk is restored.	The entire disk is restored. Each sector is restored only once.
Virtual Compatibility RDM	All disk sectors are backed up.	Only changed disk sectors are backed up.	The entire disk is restored.	The entire disk is restored. Each sector is restored only once.
Network File System (NFS)	All disk sectors are backed up.	Only changed disk sectors are backed up.	The entire disk is restored.	The entire disk is restored. Each sector is restored only once.

4.1.1.b Available Non-CBT Backup Types

The Plug-in *for VMware* always performs a Full Backup of the virtual disks for virtual machines that do not support CBT.

Important: Regardless of the disk provisioning type, non-CBT backups always back up the full disk size. Thus, backup of a 20GB thin-provisioned disk that only uses 2GB results in a 20GB backup. When you restore a non-CBT backup, all blocks are restored and allocated. After a disk is restored from a non-CBT backup, subsequent CBT-enabled Full Backups back up the entire disk.

4.1.2 File-Level Backups

The Plug-in *for VMware* can also be used to back up individual files and folders for Windows-based Guest OS. File-level backups enable granular restores of one or more files, and can be used in the event of data loss due to user errors, data corruption, or accidental deletion of files.

The Plug-in *for VMware* uses Quest NetVault Backup Plug-in *for FileSystem* (Plug-in *for FileSystem*) for performing file-level backups.

4.1.2.a Available File-Level Backup Types

The Plug-in *for VMware* supports the following types of file-level backups of virtual machines.

Note: Only the Windows version of the Plug-in *for VMware* supports file-level backups of virtual machines.

- **Full Backup** – A Full Backup backs up all selected files and directories. Full backups take longer to complete and consume more backup media. However, restores are faster since the plug-in only requires to restore a single saveset. Full Backups serve as the baseline backups for subsequent Incremental and Differential Backups.
- **Differential Backup** – A Differential Backup backs up files that are new or have changed since the last Full Backup. Differential Backups speed up recovery since the plug-in only is only required to restore two savesets. However, they consume more storage space and take longer than the Incremental Backups. Differential Backups duplicate the data backed up by previous backups of the same type.
- **Incremental Backup** – An Incremental Backup backs up files that are new or have changed since the last Full or Incremental Backup. Incremental Backups consume minimum storage space and are quicker to perform. However, data recovery takes longer and may require the plug-in to access several savesets depending on the number of incremental savesets that must be restored.

4.2.0 Defining a Backup Strategy

A well-designed backup strategy helps you recover from the damages caused by failure and resume normal operations as quickly as possible. Before you start using the plug-in for backing up data, ensure that a good backup plan is in place that protects your data from different failure modes, like media failure, accidental deletion of disk files, data corruption, or complete loss of a data centre. Typically, your backup plan should include the frequency of backups, the retention period for backups and media rotation policies, and how you will store the backup media. Answering the following questions will help you determine your data backup and storage requirements:

- How many virtual machines need protection?
- What is the amount of data to be backed up?
- Does it comprise mainly of large files or smaller ones?
- What is the frequency of updates and changes?

- Are some files updated more frequently than others?
- Are the changes confined to a small or large number of files?
- Are there situations that demand ad-hoc backups independent of regular backup schedule?
- How much space is available for storing backups and what are the future expansion plans?
- What are your off site data storage plans?

Consider your requirements, and balance your needs with costs, resources, and other factors. Include the plug-in's inherent job scheduling, media rotation, and data duplication capabilities to protect your data and create copies for local and off site storage.

4.2.1 Examples

This section provides some example backup sequences for image-level and file-level backups of virtual machines.

- ***Full Backups Only***

  A strategy comprising "Full Backups Only" can only be considered if the amount of data to be backed up is small or storage media is not a constraint. In such scenarios, you can schedule Full Backups every night, or every <n> hours depending on the frequency of updates. In the event of a failure, the plug-in is only required to restore a single saveset.

- ***Full + Differential Backups***

  For quicker restores and reduced media usage, choose a "Full + Differential" backup strategy. For example, schedule Full Backups every Sunday and Differential Backups every day or every <n> hours depending on the frequency of updates.

  In the event of a failure, the plug-in is required to restore data from the recent Full Backup and the last Differential Backup.

- ***Full + Incremental Backups***

  For quicker backups and/or minimum use of storage media, choose a "Full + Incremental" backup strategy. For example, schedule Full Backups every Sunday and Incremental Backups every day or every <n> hours depending on the frequency of updates.

  In the event of a failure, the plug-in is required to restore data from the recent Full backup and each Incremental Backup in the series. For example, if a failure occurs on Saturday, the plug-in is required to restore the Full Backup taken on Sunday and Incremental Backups taken from Monday through Friday.

Chapter 5:

PERFORMING IMAGE-LEVEL BACKUPS

- Performing Image-Level Backups
  - Selecting Data for a Backup
    - Important Notes
    - Selection Tree Icons
    - Using Backup Selection Sets
  - Setting Backup Options
    - Selecting the Backup Type
    - Enabling Changed Block Tracking
    - Generating File-Level Indexes
    - Enabling Active Block Mapping
    - Configuring Number of Parallel Streams
  - Finalizing and Submitting a Job
    - Monitoring Job Progress
- Additional Notes
  - Considerations for RDM Disks
  - Disabling CBT for a Virtual Machine

5.1.0 Performing Image-Level Backups

The procedure for performing an image-level backup includes the steps outlined in the following sections:

- Selecting Data for a Backup
- Setting Backup Options
- Finalizing and Submitting a Job

5.1.1 Selecting Data for a Backup

To select data for a backup, follow these steps:

1. Open the **NVBU Backup** window on the NVBU Server. To open this window:
   - Click **Backup** on the toolbar or **Large Buttons** panel.
   - Alternatively, on the **Operations** menu, click **Backup**.

2. On the **Selections** tab, open the NVBU Client. To open any node on the **Selections** tab:
   - Double-click the node
   - Alternatively, right-click the node, and then select **Open**
3. In the list of plug-ins, open **VMware Plugin**.
4. Open the ESX/ESXi or vCenter Server node.
5. Depending on your VMware setup and inventory view type, open the applicable nodes in the hierarchy, and select the data to be backed up. Data selection is possible at all levels starting from the Datacenter node.
   - **Hosts and Clusters Inventory View**

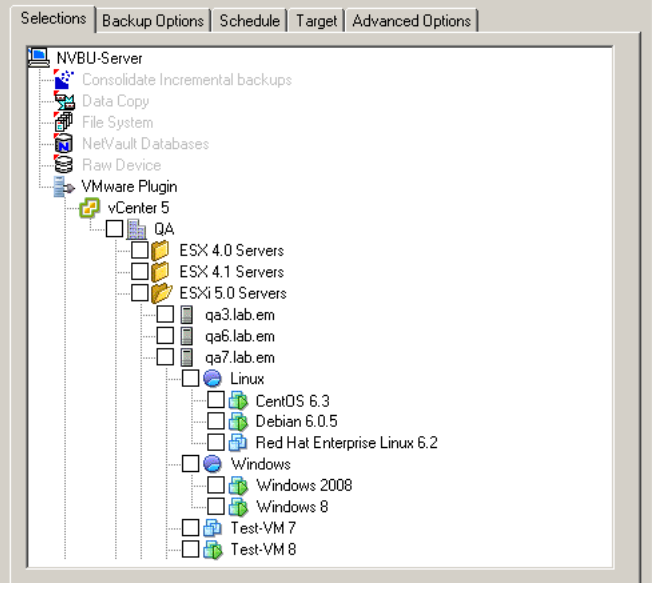


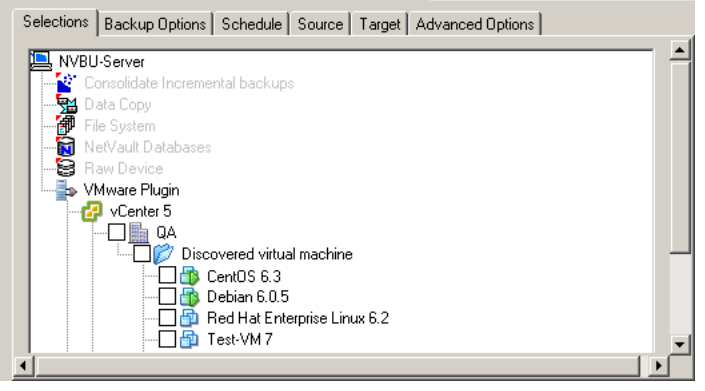
Figure 5-1: *Selections tab for Image-Level Backups – Hosts and Clusters View*

   - **Cluster Setup Managed by a vCenter Server**
     - **Back Up All Virtual Machines within a Parent Node** – Select the parent node. For example, to back up all virtual machines within a datacenter, select the Datacenter node; to back up all virtual machines within a resource pool, select the corresponding resource pool node.
     - **Back Up Individual Virtual Machines** – Depending on your virtual infrastructure, open the vCenter, Datacenter, Cluster, Resource Pool, and vApp nodes. Select the virtual machines to be backed up.

- **Standalone ESX/ESXi Server Setup**
  - **Back Up All Virtual Machines on a Host** – Select the host node.
  - **Back Up Individual Virtual Machines** – Open the ESX/ESXi Server, and select the virtual machines to be backed up.

- **VMs and Templates View** – Open the Datacenter Server, if applicable.

Figure 5-2: *Selections tab for Image-Level Backups – VMs and Templates View*



  - **Back Up All Virtual Machines in a Folder** – Select the folder node.
  - **Back Up Individual Virtual Machines** – Open the applicable folder node, and select the virtual machines to be backed up.

Note: To switch between the two views, right-click the server node, and select **Toggle Inventory View**. This command is only available when server node is open.

5.1.1.a Important Notes

- When you select the parent ESX/ESXi Server, the plug-in automatically includes the new virtual machines that are added to the host after a job has been defined. Similarly, the plug-in excludes the virtual machines that have been removed from the host. You do not have to modify the job definition each time a virtual machine is added to or removed when you select the parent ESX/ESXi Server.
- If a selected virtual machine is moved to another host using vMotion after the backup job has been defined, it will continue to be backed up as part of that job only if the following requirements are met:
  - A vCenter Server has been added to the plug-in, and the access to the virtual machine is being authenticated through the vCenter Server.
  - The ESX Server Host to which the selected virtual machine has been moved to is also controlled by the same vCenter Server.

  If these requirements are not met, the plug-in will fail to back up the virtual machine that has been moved.

- If Fault Tolerance (FT) is enabled for a virtual machine, the plug-in will not allow you to select it for a backup.

  If this feature is enabled after including a virtual machine in a backup job, the plug-in will not back it up. For such virtual machines, the following message will be added to the job logs: **"Cannot backup VM – Fault Tolerance is enabled for the VM."**
- You can select virtual machines that are part of a Virtual Application (vApp) along with the other virtual machines. Currently, the plug-in does not provide any indicators on the **Selections** tab to distinguish between such virtual machines from other virtual machines that are not part of a vApp.
- If you select a vApp node, only the virtual machines comprising the vApp are backed up. The metadata for the vApp is not included in the backup.

5.1.1.b Selection Tree Icons

Icon	Represents
	vCenter Server
	Datacenter Server
	ESX/ESXi Server Cluster
	Closed Folder
	Open Folder
	ESX/ESXi Server
	ESX/ESXi Server in Maintenance Mode
	Inaccessible ESX/ESXi Server
	Virtual Appliance (vApp)
	Resource Pool

Icon	Represents
	Virtual Machine (Powered On)
	Inaccessible Virtual Machine
	Mounted Virtual Machine
	Suspended Virtual Machine
	Powered Off Virtual Machine
	Primary Virtual Machine (Powered On) in a Fault Tolerant Group
	Inaccessible Primary Virtual Machine
	Suspended Primary Virtual Machine
	Powered Off Primary Virtual Machine
	Secondary Virtual Machine in a Fault Tolerant Group
	Inaccessible Secondary Virtual Machine
	Suspended Secondary Virtual Machine
	Powered Off Secondary Virtual Machine

5.1.1.c Using Backup Selection Sets

A Backup Selection Set lets you save frequently selected data into a composite set and use it for future backup jobs. Backup Selection Sets eliminate the need to manually select the data each time a backup is performed, and ensure that the same data set is selected for the subsequent backups. For more information about Backup Selection Sets, refer to the *Quest NetVault Backup Administrator's Guide*.

Creating a Backup Selection Set

To create a Backup Selection Set, follow these steps:

1. On the **Selections** tab, select the data to be backed up, and then in the **Backup Selection Set** area, click **Save As**.
2. In the **Save Backup Selection Set** window that appears, enter a name for the set.
3. Click **OK**.

Loading a Selection Set

To load a Backup Selection Set, follow these steps:

1. Select the **Selections** tab, and then in the **Backup Selection Set** area, click **Load**.
2. In the **Load Backup Selection Set** window that appears, select the applicable set.
3. Click **OK**.

5.1.2 Setting Backup Options

This step includes the tasks outlined in the following sections:

- Selecting the Backup Type
- Enabling Changed Block Tracking
- Generating File-Level Indexes
- Enabling Active Block Mapping
- Configuring Number of Parallel Streams

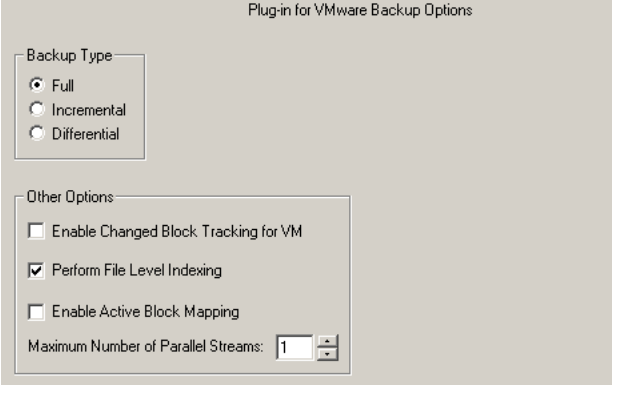


Figure 5-3: *Backup Options for Image-Level Backups*

5.1.2.a Selecting the Backup Type

Click the **Backup Options** tab, and configure the following parameter:

- **Backup Type** – Under **Backup Type**, select the applicable option:
  - **Full**
  - **Incremental**
  - **Differential**

  For more information about backup types, see *Image-Level Backups*.

Important Notes

After reverting to a snapshot that is older than its last Incremental Backup, you must perform a Full Backup of that virtual machine before performing Incremental Backups again. If you perform an Incremental Backup after a snapshot revert operation, the following error will occur:

- **vSphere 4.0** – On vSphere 4.0, the Incremental Backups include only those disk sectors that have changed since the last Incremental Backup instead of the sectors that have changed since the virtual machine was reverted. This can result in data corruption or data loss without your knowledge as vSphere does not report this error. The jobs can succeed or fail, and in some cases succeed after multiple retries. Therefore, it is necessary to avoid this situation.
- **vSphere 4.1 and Later** – On vSphere 4.1 and later, the job reports a filefault error and fails.

For more information, refer to http://kb.vmware.com/kb/1021607.

5.1.2.b Enabling Changed Block Tracking

Under **Other Options**, configure the following parameter for Full Backups:

- **Enable Changed Block Tracking for VM** – By default, CBT is disabled for a virtual machine. If you want to perform Incremental or Differential Backups of virtual machines, you must enable CBT for the Full Backup that will server as the baseline backup for the subsequent Incremental and Differential Backups.

  To enable CBT, select the **Enable Changed Block Tracking for VM** check box. The plug-in will check for this setting on the virtual machine, and if it is not enabled, reconfigure the virtual machine to enable tracking. CBT can only be enabled for virtual machines that support change tracking. Before selecting the check box, make sure that the following conditions are met:
  - The target virtual machines are managed by ESX/ESXi 4.0 or later.
  - The virtual hardware version is 7 or later.

  A log message will be issued, if the plug-in is unable to change the CBT setting for a virtual machine for any reason.

Important Notes

- During the first Full Backup that is run with the **Enable Changed Block Tracking for VM** option selected, the target virtual machine must be powered off. During the subsequent Full, Incremental, or Differential Backups, the virtual machine can remain powered on.
- At the time of enabling CBT, no snapshots should exist on a virtual machine. For more information, refer to http://kb.vmware.com/kb/1033816.
- The re-configuration of this parameter will take effect only after the virtual machine goes through a stun/unstun cycle, including power on, resume after suspend, migrate, or snapshot create, delete, or revert operations.
- During an Incremental or Differential Backup, the plug-in will not attempt to enable CBT for any virtual machine included in the backup, unless you have selected the **Enable Change Block Tracking for VM** check box for the job.
- If a new virtual machine is included in a Backup Selection Set after the initial Full or any subsequent Incremental or Differential Backup (for example, the Selection Set is modified to include a new virtual machine, or a new virtual machine is added to the ESX Server included in a Selection Set), the plug-in will do the following:
  - Create a Full Backup of the new virtual machine if you run an Incremental or Differential Backup after adding the virtual machine.
  - Create a non-CBT Full Backup, unless CBT is already enabled for the virtual machine or you have selected the **Enable Change Block Tracking for VM** check box on the **Backup Options** tab for the Incremental or Differential Backup.
  - Perform the subsequent backups of the new virtual machine as Incremental/Differential or Full depending on whether CBT is enabled or not, and a Full Backup has been performed with CBT or not.
- Once you enable CBT for a virtual machine, all subsequent Full, Incremental, and Differential Backups will be performed as CBT-based backups for that virtual machine. You do not have to select the **Enable Changed Block Tracking for VM** check box for each job.

  To stop using CBT, you must disable this feature. For instructions, see *Disabling CBT for a Virtual Machine*.
- If you perform a Full Backup of a Thick Provisioned Lazy Zeroed disk without enabling CBT, the data in the empty sectors will be converted to actual zeros during backup. When you restore the backup, the disk type will change to Eager Zeroed.

5.1.2.c Generating File-Level Indexes

When you perform an image-level backup, the plug-in automatically generates file-level indexes for all supported volumes that are included in the backup snapshot. This allows you to restore individual files and directories from an image-level backup. To enable or disable file-level indexing, configure the following parameter on the **Backup Options** tab:

- **Perform File Level Indexing** – The **Perform File Level Indexing** check box is selected by default. It allows file-level restores from Full, Incremental, and Differential image-level backups of virtual machines.

  File-level indexing is available to volumes that use the following file systems:

  - Windows – NTFS
  - Linux/UNIX – EXT2, EXT3, EXT4

  The Plug-in *for VMware* also supports volumes managed by Logical Volume Manager (LVM) on Linux-based systems and Logical Disk Manager (LDM) on Windows-based systems as single or spanned disks.

  The current version of the plug-in does not support Windows Server 2012 ReFS (Resilient File System), GPT (GUID Partition Table), and Striped Disks.

  File-level indexing does not affect the backup size. However, it increases the backup index size and the total backup time. The amount of time taken to perform file-level indexing depends on several factors, including the number of files, fragmentation of files on the volumes, network traffic, and load on the ESX or vCenter Server.

  If you do not want to use image-level backups for file-level restores, clear the **Perform File Level Indexing** check box.

5.1.2.d Enabling Active Block Mapping

The Active Block Mapping (ABM) technology provides filters to remove unused blocks during backups, which reduces the backup size and the amount of data transferred over the network. You can use ABM in conjunction with CBT to back up only active and changed blocks during Incremental and Differential Backups.

Currently, ABM is only supported for the NTFS file system on basic disks.

To enable or disable ABM during a backup, configure the following parameter on the **Backup Options** tab.

- **Enable Active Block Mapping** – ABM is disabled by default. Selecting this check box enables ABM, which allows the plug-in to back up only those sections of the virtual disks that are active. ABM scans the disk and detects inactive blocks; these blocks are then omitted during backups.

  ABM also removes deleted data. If a virtual machine backed up using ABM is restored, undelete operations will not be possible.

Note: Without Active Block Mapping, CBT will include the deleted blocks.

You can enable ABM for jobs that include both NTFS disks and non-NTFS disks, but it will only be applied to NTFS disks.

5.1.2.e Configuring Number of Parallel Streams

By default, the Plug-in *for VMware* generates a single data stream for a backup job, and backs up the selected virtual machines in a sequential manner. To increase throughput and reduce overall backup time for image-level backups, you can configure the plug-in to perform parallel backups of multiple virtual machines. To enable parallel backups, configure the following parameter on the **Backup Options** tab.

- **Maximum Number of Parallel Streams** – This parameter determines the maximum number of parallel data streams that can be generated for an image-level backup job. For example, if ten virtual machines are selected in a single job and you set this parameter to 4, the plug-in tries to back up four virtual machines in parallel.

  The actual number of parallel streams for a job depends on the following factors:

  - The number of backup devices or streams available to the backup job. For example, if you set this parameter to 4 and only two tape drives are available or an NVSD device can only support two concurrent streams, the plug-in will be able to process only two virtual machines concurrently.
  - The number of virtual machines included in the job. For example, if you set this parameter to 4, and the number of virtual machines selected for backup is 3, the plug-in creates only three data streams.

  For parallel backups, the plug-in generates a master process that coordinates the overall backup, and individual worker processes that perform the actual task of backing up the virtual machines. The maximum worker processes that can be spawned for a backup job is equal to the **Maximum Number of Parallel Streams** configured for the job. The master and the worker processes are all created on the NVBU Client on which the plug-in is running.

  When a worker process acquires a backup device and creates a backup stream, it is assigned a task to back up a virtual machine. When the backup completes, the process is assigned another task if there are any more virtual machines to be backed up. Each task is assigned a Task ID. A snapshot is generated only when a virtual machine is assigned to a worker process.

  When configuring the **Maximum Number of Parallel Streams** parameter, consider the following:

  - Ensure that the value configured for this parameter does not exceed the number of backup devices or streams accessible to a job. If the available devices are insufficient, more than one worker process may try to access

and write to the same device. This can cause significant increase in the overall backup time.

- The load of running multiple processes on the NVBU Client can have a negative impact on performance.
- The load of backing up multiple virtual machines from the same datastore can increase the I/O activity on the datatsore.
- The load of backing up multiple virtual machine that are managed by the same ESX Server can increase the load on the host if you are using the LAN Transport mode (nbd/nbdssl) for data transfer.

Note: Backup jobs created with a pre-2.5 version of the plug-in will continue to be backed up sequentially.

5.1.3 Finalizing and Submitting a Job

To finalize and submit a backup job, follow these steps:

1. Click the **Schedule**, **Target**, and **Advanced Options** tabs, and configure the required options. These options are common to all NetVault Backup Plug-ins. For more information about options, refer to the *Quest NetVault Backup Administrator's Guide*.
2. In **Job Title**, enter a title for the job. Specify a detailed title that allows you to easily identify the job for monitoring its progress or restoring data.
3. Click **Submit** on the toolbar. Alternatively, on the **Accept** menu, click **Submit Backup**.

   You can monitor the job progress from the **NVBU Jobs** window, and view the logs from the **NVBU Logs** window. For more information about these functions, refer to the *Quest NetVault Backup Administrator's Guide*.

5.1.3.a Monitoring Job Progress

To monitor progress of a job, follow these steps:

1. Open the **NVBU Jobs** window. To open this window:
   - Click **Job Management** on the toolbar or **Large Buttons** panel.
   - Alternatively, on the **Operations** menu, click **Job Management**.
2. On the **Status** tab, double-click an active job, or right-click and select **Monitor Job**.
3. The **Job Monitor** window displays the following information:
   - **Job Information**
     - **Job Title** – The title assigned to the job
     - **Job ID** – The number assigned to the job
     - **Instance** – The current instance of the job

- **Status** – The current status of the job

- **Data Transfer Details**
  - **Plugin Type** – Name of the plug-in
  - **Elapsed Time** – Total time elapsed since the job started
  - **Virtual Machines Complete** – Number of virtual machines backed up against the total virtual machines assigned to the job
- **Transfer Statistics**
  - **ID** – Task ID assigned to the worker process.
  - **Virtual Machine** – Name of the virtual machine that is being backed up
  - **Status** – Current status of the worker process
  - **Xfer Rate** – Current data transfer rate (in KB/sec)
  - **Job Size** – The size of the virtual machine (in KB, MB, GB, or TB)
  - **Progress** – Percentage of data transferred

4. After you finish reviewing the job progress, click **OK** to close the window.

5.2.0 Additional Notes

5.2.1 Considerations for RDM Disks

The Plug-in *for VMware* handles the backup and restore of RDM disks as follows:

RDM Compatibility Mode	VADP Backups and Restores
Physical Compatibility Mode	The disk is not backed up. Warning messages are written to the NVBU binary logs and job logs.
Virtual Compatibility Mode (Independent Disks)	The disk is not backed up. Warning messages are written to the NVBU binary logs and job logs.
Virtual Compatibility Mode	The disk is backed up, but the data can only be restored to a flat file. Warning messages about the change in type are written to the NVBU binary logs and job logs. Optionally, you can omit the RDM disks in virtual compatibility mode during a restore. To omit the disks, edit the **vmware.cfg** file, and set the value for **[Custom:RestoreRDMDisks]** parameter to false.

5.2.2 Disabling CBT for a Virtual Machine

To disable CBT for a virtual machine, follow these steps:

1. Power off the virtual machine.
2. In the virtual machine's configuration (**.vmx**) file, edit the following entry and set it to **"False"**:

   ```
   ctkEnabled = "False"
   ```

3. In the **.vmx** file for each virtual disk, edit the following entry and set it to **"False"**:

   ```
   scsix:x.ctkEnabled = "False"
   ```

4. Create and delete a snapshot for the virtual machine to complete a stun/unstun cycle.

Note: The **.ctk** files for the virtual machine will be automatically deleted when the virtual machine is powered on the next time.

Chapter 6:

PERFORMING FILE-LEVEL BACKUPS

- Performing File-Level Backups
  - Selecting Data for a Backup
    - Selection Tree Icons
    - Using Backup Selection Sets
  - Setting Backup Options
    - Selecting the Backup Type
    - Setting Backup Options for the Plug-in for FileSystem
  - Finalizing and Submitting a Job
- Additional Notes
  - Manually Removing the Snapshot and Mount Folder

6.1.0 Performing File-Level Backups

The procedure for performing file-level backups includes the steps outlined in the following sections:

- Selecting Data for a Backup
- Setting Backup Options
- Finalizing and Submitting a Job

6.1.1 Selecting Data for a Backup

To select data for a backup, follow these steps:

1. Open the **NVBU Backup** window on the NVBU Server. To open this window:
   - Click **Backup** on the toolbar or **Large Buttons** panel.
   - Alternatively, on the **Operations** menu, click **Backup**.
2. On the **Selections** tab, open the NVBU Client. To open any node on the **Selections** tab:
   - Double-click the node.
   - Alternatively, right-click the node, and then select **Open**.
3. In the list of plug-ins, open **VMware Plugin**.

4. Depending on your VMware setup and inventory view type, open the applicable nodes:
   - **Hosts and Clusters Inventory View** – Open the server node. Depending on your VMware setup, open the applicable nodes in the hierarchy (that is, the Datacenter, Cluster, Resource Pool, and vApp nodes) to display the available virtual machines.
   - **VMs and Templates View** – Open the server node. Depending on your VMware setup, open the applicable nodes in the hierarchy (that is the Datacenter and folder nodes) to display the available virtual machines.
5. Right-click a virtual machine, and select **Mount**.
6. The plug-in tries to obtain a snapshot of the virtual disk files and mount it on the NVBU Client. Depending on the file size of the virtual machine disk files, the mount operation can take a few minutes to complete. When the snapshot is mounted successfully, the following changes occur:
   - A folder with the same name as the selected virtual machine is created in the **Working Directory** (set in the **Configure** window).
   - A **Drives** node appears below the selected virtual machine.

Note: File-level mounting might fail if the boot disk is not the first disk among the disks attached to a virtual machine when they are ordered in **controller:device order**, that is, ide0:0, ide0:1, scsi0:0, scsi0:1, and so on.

7. Open the **Drives** node to display the available drives.
8. Select the drives, or open the nodes further to display the directory tree, and select the files and directories to be backed up.

Important: After mounting a virtual machine, you should not select the Virtual Machine node on the selection tree. If you do so, the job will fail. To include all drives in a job, you must select the drives individually.

6.1.1.a Selection Tree Icons

Icon	Represents
	vCenter Server
	Datacenter Server
	ESX/ESXi Server Cluster

Icon	Represents
	Closed Folder
	Open Folder
	ESX/ESXi Server
	ESX/ESXi Server in Maintenance Mode
	Inaccessible ESX/ESXi Server
	Virtual Appliance (vApp)
	Resource Pool
	Virtual Machine (Powered On)
	Inaccessible Virtual Machine
	Mounted Virtual Machine
	Suspended Virtual Machine
	Powered Off Virtual Machine
	Primary Virtual Machine (Powered On) in a Fault Tolerant Group
	Inaccessible Primary Virtual Machine
	Suspended Primary Virtual Machine
	Powered Off Primary Virtual Machine
	Secondary Virtual Machine in a Fault Tolerant Group

Icon	Represents
	Inaccessible Secondary Virtual Machine
	Suspended Secondary Virtual Machine
	Powered Off Secondary Virtual Machine

6.1.1.b Using Backup Selection Sets

A Backup Selection Set lets you save frequently selected data into a composite set and use it for future backup jobs. Backup Selection Sets eliminate the need to manually select the data each time a backup is performed, and ensure that the same data set is selected for the subsequent backups. For more information about Backup Selection Sets, refer to the *Quest NetVault Backup Administrator's Guide*.

Creating a Backup Selection Set

To create a Backup Selection Set, follow these steps:

1. On the **Selections** tab, select the data to be backed up, and then in the **Backup Selection Set** area, click **Save As**.
2. In the **Save Backup Selection Set** window that appears, enter a name for the set.
3. Click **OK**.

Loading a Selection Set

To load a Backup Selection Set, follow these steps:

1. Select the **Selections** tab, and then in the **Backup Selection Set** area, click **Load**.
2. In the **Load Backup Selection Set** window that appears, select the applicable set.
3. Click **OK**.

6.1.2 Setting Backup Options

This step includes the tasks outlined in the following sections:

- Selecting the Backup Type
- Setting Backup Options for the Plug-in for FileSystem

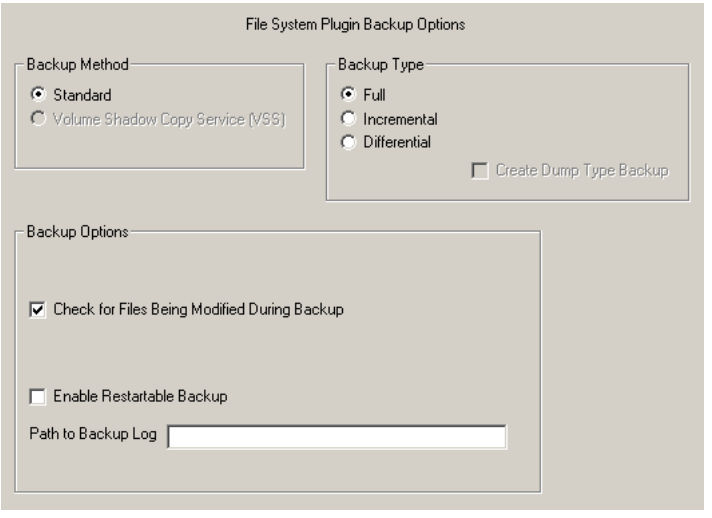


***Figure 6-1:** Backup Options for File-Level Backups*

6.1.2.a Selecting the Backup Type

Click the **Backup Options** tab, and configure the following parameters:

Note: For file-level backups, the **Standard** Backup Method is selected by default. The **Volume Shadow Copy Service (VSS)** backup method is not available to the Plug-in *for VMware*.

- **Backup Type** – Under **Backup Type**, select the applicable option:
  - **Full**
  - **Incremental**
  - **Differential**

  For more information about backup types, see *File-Level Backups*.
- **Create Dump Type Backup** – To create Dump Type Incremental or Differential Backups, select this check box. With these backups you can only restore those files that were backed up in a particular Incremental or Differential Backup.

  The **Create Dump Type Backup** check box cannot be selected for Full Backups.

6.1.2.b Setting Backup Options for the Plug-in *for FileSystem*

Under **Backup Options**, configure the following parameters:

- **Check For Files Being Modified During Backup** – By default, the plug-in will mark the files that are being updated during a backup. During restore these files will not be restored automatically. To restore these files, you must select the option **Restore Files Modified During Backup**.

  If you do not want to mark the files that are being updated during a backup, clear this check box.
- **Enable Restartable Backup** – To add the ability to stop a job and resume it later from that point, select this check box. When you stop the job, the plug-in will generate an index for all files that have been processed up to that point and write the index to the backup media and the NVDB. When you restart the job later, the plug-in will run an Incremental Backup job to back up the remaining files and folders. You can stop and restart a backup from the **NVBU Jobs** window. For more information, refer to the *Quest NetVault Backup Administrator's Guide*.

  This option can only be selected for jobs that use a Backup Selection Set.
- **Path to Backup Log** – To generate a backup log file, enter the file name. The log will provide a list of all files that are selected for a backup. The files that are backed up successfully will be marked with an **"o"** while the others will be marked with an **"x"**. You can use this option with an Incremental Backup to determine which new or changed files have been actually backed up. If you specify an existing file name, the Plug-in *for FileSystem* will overwrite the file. The backup log uses the CSV file format, and includes details such as file size, date modified, and file type.

6.1.3 Finalizing and Submitting a Job

To finalize and submit a backup job, follow these steps:

1. Click the **Schedule**, **Target**, and **Advanced Options** tabs, and configure the required options. These options are common to all NetVault Backup Plug-ins. For more information about these options, refer to the *Quest NetVault Backup Administrator's Guide*.
2. In **Job Title**, enter a title for the job. Specify a detailed title that allows you to easily identify the job for monitoring its progress or restoring data.
3. Click **Submit** on the toolbar. Alternatively, on the **Accept** menu, click **Submit Backup**.

   You can monitor the job progress from the **NVBU Jobs** window, and view the logs from the **NVBU Logs** window. For more information about these functions, refer to the *Quest NetVault Backup Administrator's Guide*

6.2.0 Additional Notes

6.2.1 Manually Removing the Snapshot and Mount Folder

When you mount a virtual machine for a file-level backup or browse, the plug-in takes the following actions:

- Creates a snapshot named BKB_SNAP for the virtual machine.
- Creates a mount folder with the same name as the virtual machine in the **Working Directory** for the plug-in.

The cleanup process automatically removes the mount folder and the snapshot when the virtual machine is unmounted. In a normal scenario, do not remove this folder or the snapshot manually.

However, if the plug-in fails to remove the mount folder or the snapshot for any reason, a subsequent mount of the same virtual machine will fail with the error "A stale mount was found". For example, this could happen if the plug-in exits unexpectedly after mounting a virtual machine. In this scenario, you must manually remove the mounted disks and the snapshot. You must also complete these steps if a snapshot is inadvertently deleted manually while a virtual machine is still mounted.

To manually remove the snapshot and mount folder, follow these steps:

1. If **nvvmwmount.exe** is running, unmount the virtual machines that are currently mounted for browse or backup. Stop the NVBU Service. This step is only applicable to v2.1.55 and prior releases of the Plug-in *for VMware*.
2. If the mount folder for the virtual machine is present in the **Working Directory**, remove it.
3. If you were using an advanced transport mode, such as san or hotadd, navigate to the **<system_drive>/windows/temp/vmware-system** directory. If this directory contains any sub-directory named **<VM_UUID>-<VMmoref>** (where **<VM_UUID>** is the UUID of the mounted virtual machine and **VM_moref** is an internal reference that the ESX or vCenter Server uses to refer to the virtual machine), delete it. To delete this folder, you may be required to set the necessary permissions for the folder.
4. If you were using the hotadd transport mode, remove any disks of the target virtual machine (the virtual machine mounted for a backup) that were hotadded to the NVBU Client Virtual Machine (the virtual machine where the Plug-in *for VMware* is running). This can be done from the vSphere Client for the virtual machine where the Plug-in/NVBU Client is running.
5. Go to the Snapshot Manager in vSphere Client, and remove the BKB_SNAP snapshot, if it is still available. Wait for a few minutes (approximately 2-3 minutes) to allow any memory cache to be cleared before performing this step.

If the virtual machine is powered on, an error message **“Unable to access file <unspecified filename> since it is locked”** may appear when you try to delete the snapshot, but the snapshot may thereafter disappear from the Snapshot Manager window. If a **“Consolidate Helper-0”** snapshot appears after you remove the snapshot, power off the virtual machine.

6. VMware recommends that you create and delete a snapshot at this point. You can do this from the Snapshot Manager window in vSphere Client. Note that the server tries to consolidate the redo logs during this operation, and therefore, it may take a few minutes. Delete the Consolidate Helper snapshot, if present.
7. If some unwanted redo logs are still present on the datastore, perform step 6 again. Wait for a few minutes (approximately 2-3 minutes) to allow any memory cache to be cleared before performing this step.

Chapter 7:

RESTORING IMAGE-LEVEL BACKUPS

- Available Restore Types for Image-Level Backups
- Recovering a Full Virtual Machine from Image-Level Backups
  - Prerequisites
  - Selecting Data for a Restore
    - Selection Tree Icons
  - Setting Restore Options
    - Selecting the Restore Method
    - Setting Virtual Machine Recovery Options
  - Finalizing and Submitting a Job
- Advanced Restore Procedures
  - Relocating a Virtual Machine to an Alternate ESX Server Host
  - Renaming a Virtual Machine During Restore
- Performing File-Level Restores from Image-Level Backups
  - Selecting Data for a Restore
    - Selection Tree Icons
  - Setting Restore Options
    - Selecting the Restore Method
    - Setting Virtual Machine File Restore Options
  - Finalizing and Submitting a Job
- Restoring Virtual Machine Disk and Configuration Files
  - Selecting Data for a Restore
    - Selection Tree Icons
  - Setting Restore Options
    - Selecting the Restore Method
    - Setting Virtual Machine File Restore Options
  - Finalizing and Submitting a Job
  - Recovering a Virtual Machine From the Restored Files
    - Recovering a Virtual Machine from a VCB Backup

- Recovering a Virtual Machine from a VADP Backup using vCenter Converter
- Additional Features Available on the Selections Tab

7.1.0 Available Restore Types for Image-Level Backups

The image-level backups can be used to perform the following types of restores:

- **Recover a Full Virtual Machine** – The image-level backups let you recover a virtual machine to a previous known state in the event of hardware failure or accidental deletion of virtual machine disk files. These backups can be used to restore an entire virtual machine to the same or an alternate ESX Server Host.
- **Restore Individual Files and Directories** – Starting with version 2.2, you can use the image-level backups to restore individual files and directories to a specified directory on the NVBU Client. File-level restores can be used in the event of data loss due to user errors, data corruption, or accidental deletion of files.

  File-level restores are supported on the following file systems:

  - Windows – NTFS
  - Linux/UNIX – EXT2, EXT3, EXT4

  The Plug-in *for VMware* also supports volumes managed by Logical Volume Manager (LVM) on Linux-based systems and Logical Disk Manager (LDM) on Windows-based systems as single or spanned disks.

  The current version of the plug-in does not support Windows Server 2012 ReFS (Resilient File System), GPT (GUID Partition Table), and Striped Disks.

Note: To use an image-level backup for file-level restores, you must have selected the **Perform File Level Indexing** check box during backup.

- **Restore Virtual Machine Disk and Configuration Files** – The image-level backups can be used to restore the virtual machine disk and configuration files to a specified directory on the NVBU Client. The restored files can then be used to recover a virtual machine with the same or modified settings using the Virtual Infrastructure Client or any other available utility that allows you to create a new virtual machine using the existing **.vmdk** files.

7.2.0 Recovering a Full Virtual Machine from Image-Level Backups

The procedure for recovering a full virtual machine from an image-level backup includes the step outlined in the following sections:

- Prerequisites
- Selecting Data for a Restore
- Setting Restore Options
- Finalizing and Submitting a Job
- Starting the Virtual Machine

7.2.1 Prerequisites

Before you start the restore procedure, make sure that the following requirements are met:

- If the virtual machine to be restored still exists on the host server, delete it.

7.2.2 Selecting Data for a Restore

To select data for a restore, follow these steps:

1. Open the **NVBU Restore** window on the NVBU Server. To open this window:
   - Click **Restore** on the toolbar or **Large Buttons** panel.
   - Alternatively, on the **Operations** menu, click **Restore**.
2. On the **Selections** tab, open the NVBU Client. To open any node on the **Selections** tab:
   - Double-click the node
   - Alternatively, right-click the node, and then select **Open**
3. In the list of plug-ins, open **VMware Plugin** to display the backup savesets created with the plug-in. Each saveset will be labeled with its job title followed by the saveset ID and the backup timestamp.
4. Open the applicable saveset. From this level, double-click a node to open it (the right-click + **Open** method is not available).
5. Open the vCenter, Datacenter, ESX Host Cluster and the ESX Server to list the VMware images stored in the saveset.
6. Select the images to be restored.

Important Notes

- For an image-level restore, if you select any file or directory under the **Volumes** node, the job will fail.
- If you select an Incremental or a Differential Backup, the plug-in will automatically restore all savesets in the backup sequence up to the selected saveset. The plug-in will not perform any unnecessary steps to read, send, or write sectors that have changed in a later backup. Each sector will be restored only once.

7.2.2.a Selection Tree Icons

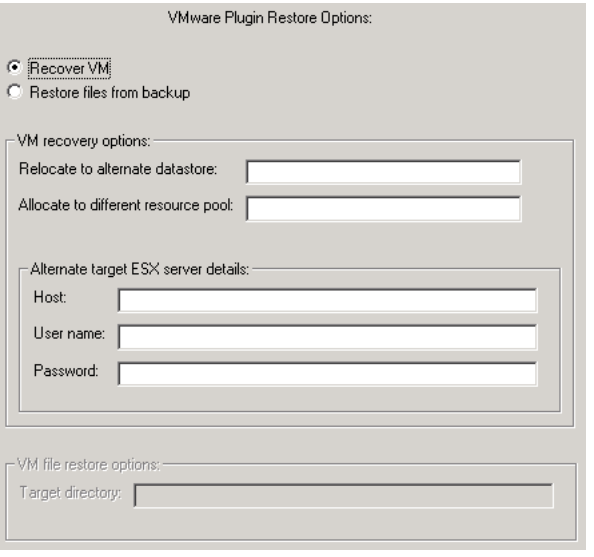
Icon	Represents
	Virtual Machine
	Configuration File
	NVRAM File
	Virtual Machine Disk File
	Disk Extent Information File
	Log File
	Catalog File

7.2.3 Setting Restore Options

This step includes the tasks outlined in the following sections:

- Selecting the Restore Method
- Setting Virtual Machine Recovery Options

Figure 7-1: *Restore Options for Image-Level Backups*



7.2.3.a Selecting the Restore Method

Click the **Restore Options** tab, configure the following parameter:

- **Recover VM** – Select the **Recover VM** option to restore an entire virtual machine.

7.2.3.b Setting Virtual Machine Recovery Options

If you need to change the datastore or resource pool for a virtual machine, configure the following parameters under **Recovery Options**:

- **Relocate to Alternate Datastore** – A datastore represents a storage location for virtual machine files, which can be a VMFS volume, a directory on Network Attached Storage, or a local file system path. A datastore is platform-independent and host-independent.

  To change the datastore for a virtual machine, enter the destination datastore name for the virtual machine in **Relocate to Alternate Datastore**. You can use this option when the original datastore is unavailable, inaccessible or cannot hold the virtual machine due to lack of space. Ensure that the name is correct and the datastore is accessible to the ESX Server Host.

  When you configure an alternate datastore, all the virtual disk and configuration files associated with a virtual machine are restored to a single datastore. Make sure that the target datastore has sufficient disk space to hold the virtual machine files. The restore will fail if you specify an invalid or inaccessible datastore, or if the datastore does not have sufficient space.

- **Allocate to Different Resource Pool** – A resource pool represents the CPU and memory resources available to an ESX Server host or a cluster of hosts, which in turn is made available to the individual virtual machines controlled by the host. Resource pools can be configured in terms of absolute minimum and maximum quantities, or relative shares. To run any virtual machine, it must be allocated a resource pool.

  By default, a virtual machine is allocated to its original resource pool during restore. To change this, enter the target resource pool for the virtual machine in **Allocate to Different Resource Pool**. Use the following format to specify the resource pool:

  /PoolA/PoolB/.../Pool<n>

  where **Pool<n>** is the target resource pool. **PoolA** is the child of the root resource pool, **PoolB** is the child of **PoolA** and so on. This format allows you to specify a resource pool at any arbitrary depth within the hierarchy. To allocate the virtual machine to the root resource pool, enter **"/"**.

  Note the following:

  - If you do not specify any resource pool, the virtual machine will be allocated to its original resource pool (as at the time of backup).
  - If you specify an invalid or inaccessible resource pool, the plug-in will follow the path hierarchy backwards to find a valid resource pool, and allocate the virtual machine to the first valid ancestor pool in the path. An error message will be logged if this occurs.

Setting Additional Restore Option for Legacy Backups

For savesets created with Plug-in *for VMware* 1.x, the **Restore Options** tab provides an additional **Perform COS-Less Restore** check box.

The Plug-in *for VMware* 1.x used this parameter to determine the restore type for the image-level backups. Since the plug-in no longer supports the COS-Based and COS-Less restore types, the later versions of the plug-in ignore this option during a restore. However, this check box must be selected to specify an alternate datastore or resource pool while restoring a saveset created with 1.x. If you do not select this check box, the plug-in will ignore the settings for the **Relocate to Alternate Datastore** and **Allocate to Different Resource Pool** parameters for savesets created with Plug-in *for VMware* 1.x.

7.2.4 Finalizing and Submitting a Job

To finalize and submit a restore job, follow these steps:

1. Click the **Source**, **Schedule**, and **Advanced Options** tabs, and configure the required options. These options are common to all NetVault Backup Plug-ins. For more information these options, refer to the *Quest NetVault Backup Administrator's Guide*.

2. In **Job Title**, enter a title for the job. Specify a detailed title that allows you to easily identify the job for monitoring its progress.
3. Click **Submit** on the toolbar. Alternatively, on the **Accept** menu, click **Submit Restore**.

   You can monitor the job progress from the **NVBU Jobs** window, and view the logs from the **NVBU Logs** window. For more information about functions, refer to the *Quest NetVault Backup Administrator's Guide*.

7.2.5 Starting the Virtual Machine

After the restore, the virtual machine will be in a powered off state. You must start it manually. When you start it, the operating system might prompt for error recovery or a reason for the "unclean" shutdown. In most cases, this can be ignored and you can select to boot normally.

7.3.0 Advanced Restore Procedures

7.3.1 Relocating a Virtual Machine to an Alternate ESX Server Host

To relocate a virtual machine to an alternate ESX Server host, follow these steps:

1. Open the **NVBU Restore** window, and select the image to be restored. For more information on selecting the data, see *Selecting Data for a Restore*.
2. Click the **Restore Options** tab, and configure the Restore Method and the Virtual Machine Recovery options. For more information, see *Setting Restore Options*.
3. Under **Alternate Target ESX Server Details**, configure the following parameters:
   - **Host** – Enter the IP address or DNS name of the target ESX Server host.
   - **User Name** – Provide a user account that can be used to log on to the ESX Server. The user must have privileges to register or create virtual machines
   - **Password** – Enter the password associated with the configured user.
4. Finalize and submit the job. For more information, see *Finalizing and Submitting a Job*.

7.3.2 Renaming a Virtual Machine During Restore

To rename a virtual machine during restore, follow these steps:

1. Open the **NVBU Restore** window, and select the image to be restored. For more information on selecting the data, see *Selecting Data for a Restore*.
2. Right-click the virtual machine, and select **Rename**.

3. In the **Restore Rename** dialog, configure the following parameter:
   - **Rename To** – Select the check box, and enter a new name for the virtual machine. The name can contain a maximum of 80 characters. It cannot include any special characters (such as, / \ ? * : @ > < | " ? &). The job will fail with an error message if the virtual machine name is longer than 80 characters or uses any special character.

     Click **OK** to close the dialog. The plug-in will update the corresponding node on the **Selections** tab to display the new name for the virtual machine.

Note: The **Rename** option is only available for backups performed with plug-in version 2.6 and later.

4. Click the **Restore Options** tab, and configure the applicable parameters. For more information, see *Setting Restore Options*.
5. Finalize and submit the job. For more information, see *Finalizing and Submitting a Job*.

Note: When you rename a virtual machine, the plug-in renames all disk and configuration files except the **vmware.log** files.

6. After restore, when you try to power on the virtual machine, a message will appear asking whether you copied the virtual machine or moved it. Select the **"I copied it"** option, and click **OK** to start the virtual machine.

7.4.0 Performing File-Level Restores from Image-Level Backups

The procedure for performing file-level restores from an image-level backup includes the steps outlined in the following sections:

- Selecting Data for a Restore
- Setting Restore Options
- Finalizing and Submitting a Job

7.4.1 Selecting Data for a Restore

To select data for a restore, follow these steps:

1. Open the **NVBU Restore** window on the NVBU Server. To open this window:
   - Click **Restore** on the toolbar or **Large Buttons** panel.
   - Alternatively, on the **Operations** menu, click **Restore**.
2. On the **Selections** tab, open the NVBU Client. To open any node on the **Selections** tab:

- Double-click the node
- Alternatively, right-click the node, and then select **Open**

3. In the list of plug-ins, open **VMware Plugin** to display the backup savesets created with the plug-in. Each saveset will be labeled with its job title followed by the saveset ID and the backup timestamp.
4. Open the applicable backup saveset. From this level, double-click a node to open it (the right-click + **Open** method is not available).
5. Open the vCenter, Datacenter, ESX Host Cluster, and the ESX Server nodes to display all VMware images stored in the saveset.
6. Open the applicable image.
7. Open the **Volumes** node, and then open the disk partitions to display the directory tree.
8. Select the files and directories to be restored.

7.4.1.a Selection Tree Icons

Icon	Represents
	Virtual Machine
	Volume
	Partition
	Configuration File
	NVRAM File
	Virtual Machine Disk File
	Disk Extent Information File
	Log File
	Catalog File

7.4.2 Setting Restore Options

This step involves the tasks outlined in the following sections:

- Selecting the Restore Method
- Setting Virtual Machine File Restore Options

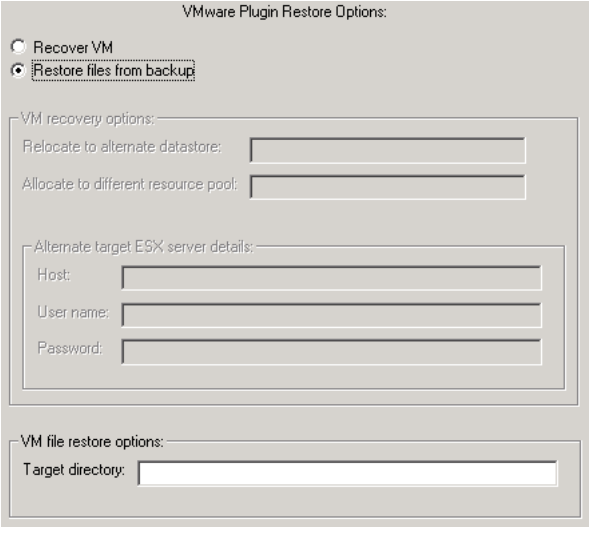


Figure 7-2: *Restore Options tab for Virtual Machine Files Only Restore Method*

7.4.2.a Selecting the Restore Method

Click the **Restore Options** tab, and configure the following parameter:

- **Restore Files from Backup** – Select the **Restore Files from Backup** option.

Important: The restore job will fail if you do not select **Restore Files from Backup** option after selecting the files and directories under the **Volumes** node.

7.4.2.b Setting Virtual Machine File Restore Options

Under **VM File Restore Options**, configure the following parameter:

- **Target Directory** – Enter the full path to the directory to which you want to restore the selected data. The target directory must be local to the NVBU Client on which the Plug-in *for VMware* is running. This release does not support mapped or mounted network shares, or UNC paths. The plug-in will not check whether the target directory is local or remote. The restore job will fail if the specified path is not accessible to the plug-in.

7.4.3 Finalizing and Submitting a Job

To finalize and submit a restore job, follow these steps:

1. Click the **Source**, **Schedule**, and **Advanced Options** tabs, and configure the required options. These options are common to all NetVault Backup Plug-ins. For more information about these options, refer to the *Quest NetVault Backup Administrator's Guide*.
2. In **Job Title**, enter a title for the job. Specify a detailed title that allows you to easily identify the job for monitoring its progress.
3. Click **Submit** on the toolbar. Alternatively, on the **Accept** menu, click **Submit Restore**.

   You can monitor the job progress from the **NVBU Jobs** window, and view the logs from the **NVBU Logs** window. For more information about these functions, refer to the *Quest NetVault Backup Administrator's Guide*.

7.5.0 Restoring Virtual Machine Disk and Configuration Files

The procedure for restoring virtual machine disk and configuration files from an image-level backup includes the steps outlined in the following sections:

- Selecting Data for a Restore
- Setting Restore Options
- Finalizing and Submitting a Job
- Recovering a Virtual Machine From the Restored Files

7.5.1 Selecting Data for a Restore

To select data for a restore, follow these steps:

1. Open the **NVBU Restore** window on the NVBU Server:
   - Click **Restore** on the toolbar or **Large Buttons** panel
   - Alternatively, on the **Operations** menu, click **Restore**.
2. On the **Selections** tab, open the NVBU Client. To open any node on the **Selections** tab:
   - Double-click the node
   - Alternatively, right-click the node, and then select **Open**
3. In the list of plug-ins, open **VMware Plugin** to display the backup savesets created with the plug-in. Each saveset will be labeled with its job title followed by the saveset ID and the backup timestamp.
4. Open the applicable backup saveset. From this level, double-click a node to open it (the right-click + **Open** method is not available).

5. Open the vCenter, Datacenter, ESX Host Cluster, and the ESX Server nodes to display the virtual machine images stored in the saveset.
6. Select the images for which you want to restore the disk and configuration files.

7.5.1.a Selection Tree Icons

Icon	Represents
	Virtual Machine
	Configuration File
	NVRAM File
	Virtual Machine Disk File
	Disk Extent Information File
	Log File
	Catalog File

7.5.2 Setting Restore Options

This step involves the tasks outlined in the following sections:

- Selecting the Restore Method
- Setting Virtual Machine File Restore Options

7.5.2.a Selecting the Restore Method

Click the **Restore Options** tab, and configure the following parameter:

- **Restore Files from Backup** – Select the **Restore Files from Backup** option.

7.5.2.b Setting Virtual Machine File Restore Options

Under **VM File Restore Options**, configure the following parameter:

- **Target Directory** – Enter the full path to the directory to which you want to restore the virtual disk and configuration files. The target directory must be local to the NVBU Client on which the Plug-in *for VMware* is running. This release does not support mapped or mounted network shares, or UNC paths. The plug-in will not check whether the target directory is local or remote. The restore job will fail if the specified path is not accessible to the plug-in.

7.5.3 Finalizing and Submitting a Job

To finalize and submit a restore job, follow these steps:

1. Click the **Source**, **Schedule**, and **Advanced Options** tabs, and configure the required options. These options are common to all NetVault Backup Plug-ins. For more information about these options, refer to the *Quest NetVault Backup Administrator's Guide*.
2. In **Job Title**, enter a title for the job. Specify a detailed title that allows you to easily identify the job for monitoring its progress.
3. Click **Submit** on the toolbar. Alternatively, on the **Accept** menu, click **Submit Restore**.

   You can monitor the job progress from the **NVBU Jobs** window, and view the logs from the **NVBU Logs** window. For more information about these functions, refer to the *Quest NetVault Backup Administrator's Guide*.

7.5.4 Recovering a Virtual Machine From the Restored Files

After restoring the virtual machine disk and configuration files, you can use the VMware vCenter Converter Standalone Client to create a new virtual machine using the restored **.vmx** and **.vmdk** files. After a VADP Recovery, you must modify the **.vmx** file so that it matches the disk paths of the restored vmdks. For more information, refer to the relevant VMware vCenter Converter Standalone Client documentation.

7.5.4.a Recovering a Virtual Machine from a VCB Backup

To recover the virtual machine files to the destination VMware Server, launch the VMware vCenter Converter Standalone Client Wizard. Follow the wizard as it takes you through the various steps. When the **"Select source type:"** prompt appears, select **"Backup image or third-party virtual machine"**. For the **"Virtual machine file"** parameter, select the restored **.vmx** file.

7.5.4.b Recovering a Virtual Machine from a VADP Backup using vCenter Converter

The **.vmx** file reflects the datastore paths of the **.vmdk** snapshot files at the time of the backup. You must edit this file to reflect the restored **.vmdk** files.

1. Navigate to the target directory to which the virtual machine files were restored and note the file names of the virtual disks.

   An example of files generated from **Virtual Machine Files Only Restore** of a VADP backup is given below:

   ```
   MyVirtualMachine.vmx
   scsi0-0-MyVirtualMachine.vmdk
   scsi0-0-MyVirtualMachine-s001.vmdk
   VirtualMachineConfigInfo
   ```

2. Open the **.vmx** file.
3. Modify the relevant entries for the virtual disk(s).

   For example, modify the following entry

   ```
   scsi0:0.fileName = "MyVirtualMachine-000001.vmdk"
   ```

   so that it matches the **.vmdk** file generated during the restore

   ```
   scsi0:0.fileName = "scsi0-0-MyVirtualMachine.vmdk"
   ```

4. After modifying the **.vmx** file, launch the VMware vCenter Converter Standalone Client Wizard to create the virtual machine. Follow the wizard as it takes you through the various steps. When the **"Select source type:"** prompt appears, select "**VMware Workstation or other VMware virtual machine"**. For the **"Virtual machine file"** parameter, select the restored **.vmx** file.

Note: In the scenario described in the article http://kb.vmware.com/kb/1019286, the **.vmx** file will not be backed up. The **.vmdk** files will still be available.

7.6.0 Additional Features Available on the Selections Tab

This section provides a brief description of the additional features available on the **Selections** tab of the **NVBU Restore** window. These features are common to all NVBU Plug-ins. For more information about these functions, refer to the *Quest NetVault Backup Administrator's Guide*.

- **Sorting the Savesets** – By default, the savesets are sorted by the plug-in name. To change the sorting order, select the applicable method in the **Selection Method** list:
  - **Plugin** – This is the default method.

- **Backup Set** – To sort the savesets by the Selection Set used for the backup, select **Backup Set** in the **Selection Method** list.
- **Job** – To sort the savesets by the Job Title, select **Job** in the **Selection Method** list.

- **Filtering the Savesets** – To filter the savesets, configure the following parameters under **Filter Options**:
  - **By Date Range** – Select the **By Date Range** check box, and enter or select the **From** and **To** dates to list the savesets generated during a given period.
  - **Show On-line Status** – Select the **Show On-line Status** check box to list the savesets stored in the currently online media items.

  Click **Apply Filter** to set the filter.
- **Searching for Data Items** – To find a data item inside a saveset, right-click it, and select **Search**. Enter the item name in **Search String**, and click **Search**.
- **Viewing Media List** – To view the media list for a saveset, right-click it, and select **Media List**.
- **Compressing Indexes** – To compress the online indexes, right-click the target client or the saveset, and select **Compress**. The index is automatically de-compressed when you open a saveset to browse or restore the data.

Chapter 8:

RESTORING FILE-LEVEL BACKUPS

- Available Restore Methods for File-Level Backups
- Restoring File-Level Backups Using Shared Network Drives
  - Setting Up a Network Share
  - Selecting Data for a Restore
  - Setting Restore Options
  - Finalizing and Submitting a Job
- Restoring File-Level Backups Using the Native Plug-in for FileSystem
  - Prerequisites
  - Restoring Data
- Additional Features Available on the Selections Tab

8.1.0 Available Restore Methods for File-Level Backups

The Plug-in *for VMware* provides the following methods for restoring file-level backups:

- **Restores Using Shared Network Drives** – This method does not require an instance of NVBU Client running inside the virtual machine. Restores are performed to the shared network drives on the virtual machines, using the Plug-in *for FileSystem* installed on the NVBU Client. Since the Plug-in *for FileSystem* is automatically installed with an NVBU Client, no additional software is required for this type of restore.
- **Restores Using Native Plug-in *for FileSystem*** – This method is suitable if an instance of NVBU Client is already running inside the virtual machine for the backup and recovery of other data. The virtual machine is treated as any other physical NVBU Client for the file system restores.

8.2.0 Restoring File-Level Backups Using Shared Network Drives

The procedure for restoring file-level backups to a shared folder on the virtual machine includes the steps outlined in the following sections:

- Setting Up a Network Share
- Selecting Data for a Restore
- Setting Restore Options
- Finalizing and Submitting a Job

8.2.1 Setting Up a Network Share

To create a network share between the NVBU Client and the target virtual machine, follow these steps:

1. On the target virtual machine, configure the sharing properties for a folder.
2. Open the **NVBU Backup** window on the NVBU Server.
3. On the **Selections** tab, open the NVBU Client.
4. In the list of plug-ins, open **File System**.
5. Right-click **Network Shares**, and select **Add Network Share**.
6. In the **Add New Network Share** window, enter the path for the shared drive in the following format:

   `\\<IP Address or Resolvable Network Name>\<Share Name>\`
7. Click **Add**. This adds the shared folder to the **Network Shares** node.
8. Right-click the shared folder, and select **Connect As**.
9. In the **Connection Details** window, configure the login details:
   - **Domain** – Enter the Windows domain for the virtual machine.
   - **Username** – Enter a user name with necessary privileges to write/change files on the shared folder.
   - **Password** – Enter the password associated with the configured user.
10. Click **OK**.

8.2.2 Selecting Data for a Restore

To select data for a restore, follow these steps:

1. Open the **NVBU Restore** window on the NVBU Server. To open this window:
   - Click **Restore** on the toolbar or **Large Buttons** panel.
   - Alternatively, on the **Operations** menu, click **Restore**.
2. On the **Selections** tab, open the NVBU Client. To open any node on the **Selections** tab:

- Double-click the node
- Alternatively, right-click the node, and then select **Open**

3. In the list of plug-ins, open **File System**. (The Plug-in *for VMware* internally uses the Plug-in *for FileSystem* to perform file-level backups of virtual machines. Therefore, the savesets for these backups are listed under the Plug-in *for FileSystem*.)

   To distinguish the savesets generated for virtual machines, the virtual machine name is appended to the Job Title. Thus, the label for the savesets contains the Job Title, followed by the virtual machine name, the saveset ID, and the backup timestamp.
4. Open the applicable backup saveset to display the directories and files included in the backup. From this level, double-click a node to open it (the right-click + **Open** method is not available).

Note: For a regular Incremental or Differential Backup, the selection tree displays all files that were included in the backup sequence (the initial Full Backup and the subsequent Incremental or Differential Backups), but for a Dump Type Incremental or Differential Backup, the plug-in only displays those files that were backed up in the selected saveset.

5. Select the files and directories to be restored.
6. Right-click a file or folder, and select **Rename**.
7. In the **Restore Rename** window, select the **Relocate To** check box, and enter the network share path.

Important: If you do not perform steps 6 and 7, the data will be restored to the NVBU Client and not the shared folder on the virtual machine.

8.2.3 Setting Restore Options

Click the **Restore Options** tab, and configure the following parameters:

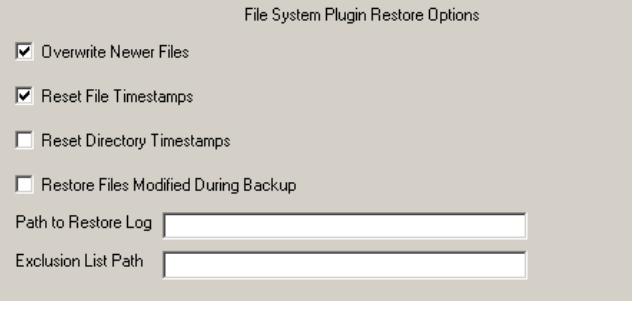


Figure 8-1: *Restore Options for File-level Restore*

- **Overwrite Newer Files** – By default, the plug-in will overwrite the existing files on the restore destination with the backed up version in the saveset.

  If you do not want to overwrite the files that are available on the restore destination, clear the check box.
- **Reset File Timestamps** – By default, the plug-in will reset the timestamps for the restored files to what is recorded in the backup saveset.

  If you want to restore the files with current timestamp, clear the check box.
- **Reset Directory Timestamps** – By default, the directory time stamps will be set to the time of the restore job.

  To reset the timestamp to what is recorded in the saveset, select this check box. You must also select the **Reset File Timestamps** check box to reset the timestamps for the restored directories to what is recorded in the backup.
- **Restore Files Modified During Backup** – To restore files that were in a modified state during a backup, select this check box.
- **Path to Restore Log** – To generate a restore log file, enter the file name. The log file will provide a list of all files that are selected for a restore. The files that are restored successfully will be marked with an **"o"** while the others will be marked with an **"x"**. If you specify an existing filename, the plug-in will overwrite the file. The restore log uses the CSV file format, and includes details such as file size, date modified, and file type.
- **Exclusion List Path** – To use an exclusion list, enter the full path to the file. For more information about Exclusion Lists, refer to *Quest NetVault Backup Plug-in for FileSystem User's Guide*.

8.2.4 Finalizing and Submitting a Job

To finalize and submit a restore job, follow these steps:

1. Click the **Source**, **Target Client**, **Schedule**, and **Advanced Options** tabs, configure the required options. These options are common to all NetVault Backup Plug-ins. For more information about these options, refer to the *Quest NetVault Backup Administrator's Guide*.
2. In **Job Title**, enter a title for the job. Specify a detailed title that allows you to easily identify the job for monitoring its progress.
3. Click **Submit** on the toolbar. Alternatively, on the **Accept** menu, click **Submit Restore**.

   You can monitor the job progress from the **NVBU Jobs** window, and view the logs from the **NVBU Logs** window. For more information about these functions, refer to the *Quest NetVault Backup Administrator's Guide*.

Important: The plug-in will restore the data to the shared network folder on the virtual machine. You must manually move the restored files to the final target destination.

8.3.0 Restoring File-Level Backups Using the Native Plug-in *for FileSystem*

The procedure for restoring the file-level backups using the native Plug-in *for FileSystem* includes the steps outlined in the following steps:

- Prerequisites
- Restoring Data

8.3.1 Prerequisites

Before you restore the data, make sure that the following requirements are met:

- Install the NVBU Client software inside the target virtual machine. For more information, refer to the *Quest NetVault Backup Installation Guide*.
- Add the client to NVBU Server. For more information, refer to the *Quest NetVault Backup Administrator's Guide*.

8.3.2 Restoring Data

To restore data to a virtual machine, follow these steps:

1. Open the **NVBU Restore** window on the NVBU Server. To open this window:
   - Click **Restore** on the toolbar or **Large Buttons** panel.
   - Alternatively, on the **Operations** menu, click **Restore**.
2. On the **Selections** tab, open the NVBU Client. To open any node on the **Selections** tab:
   - Double-click the node
   - Alternatively, right-click the node, and then select **Open**
3. In the list of plug-ins, open **File System**. (The Plug-in *for VMware* internally uses the Plug-in *for FileSystem* to perform file-level backups of virtual machines. Therefore, the savesets for these backups are listed under the Plug-in *for FileSystem*.)

   To distinguish the savesets generated for virtual machines, the virtual machine name is appended to the Job Title. Thus, the label for the savesets contains the Job Title, followed by the virtual machine name, the saveset ID, and the backup timestamp.
4. Open the applicable backup saveset to display the directories and files included in the backup. From this level, double-click a node to open it (the right-click + **Open** method is not available).

Note: For a regular Incremental or Differential Backup, the selection tree displays all files that were included in the backup sequence (the initial Full Backup and the subsequent Incremental or Differential Backups), but for a Dump Type Incremental or Differential Backup, the plug-in only displays those files that were backed up in the selected saveset.

5. Select the files and directories to be restored.
6. Click the **Restore Options** tab, and configure the required parameters. For more information, see *Setting Restore Options*.
7. Click the **Target Client** tab, and in the list of NVBU Clients, select the target virtual machine.

Important: If you do not select the virtual machine on the **Target Client** tab, the data will be restored to the NVBU Client and not the target virtual machine.

8. Finalize and submit the job. For more information, see *Finalizing and Submitting a Job*.

8.4.0 Additional Features Available on the Selections Tab

This section provides a brief description of the additional features available on the **Selections** tab of the **NVBU Restore** window. These features are common to all NVBU Plug-ins. For more information about these functions, refer to the *Quest NetVault Backup Administrator's Guide*.

- **Sorting the Savesets** – By default, the savesets are sorted by the plug-in name. To change the sorting order, select the applicable method in the **Selection Method** list:
  - **Plugin** – This is the default method.
  - **Backup Set** – To sort the savesets by the Selection Set used for the backup, select **Backup Set** in the **Selection Method** list.
  - **Job** – To sort the savesets by the Job Title, select **Job** in the **Selection Method** list.
- **Filtering the Savesets** – To filter the savesets, configure the following parameters under **Filter Options**:
  - **By Date Range** – Select the **By Date Range** check box, and enter or select the **From** and **To** dates to list the savesets generated during a given period.
  - **Show On-line Status** – Select the **Show On-line Status** check box to list the savesets stored in the currently online media items.

  Click **Apply Filter** to set the filter.

- **Searching for Data Items** – To find a data item inside a saveset, right-click it, and select **Search**. Enter the item name in **Search String**, and click **Search**.
- **Viewing Media List** – To view the media list for a saveset, right-click it, and select **Media List**.
- **Compressing Indexes** – To compress the online indexes, right-click the target client or the saveset, and select **Compress**. The index is automatically de-compressed when you open a saveset to browse or restore the data.

Chapter 9:

TROUBLESHOOTING

- Common Errors
- SOAP Messages
- VDDK Logs

9.1.0 Common Errors

This section describes some common errors and their solution.

Description	Symptom	Solution
Plug-in crashes during a backup.	During a backup, the plug-in crashes with the following error in the NVBU Logs: **Backing up data of VM disk [XXXXXXX]xxx/xxxx-xxxxx.vmdk' to media : "Job manager lost message channel unexpectedly."** The Trace Logs include the following error: **Cannot open library: libexpat.so.0: cannot open shared object file in vixDiskLib-16642.log**.	This is a Linux library problem. To correct this problem, navigate to the **/usr/lib** directory, and create the following symbolic link: **ln -s /lib/libexpat.so.1.5.2 libexpat.so.0**
CBT-based Image-level backup fails.	An image-level backup for which CBT has been enabled fails with the following error message in the NVBU Logs: **"Failed to get changed disk areas."**	This issue occurs when a snapshot already exists on a virtual machine when CBT is enabled. For snapshots that exist before enabling CBT, the **changeId** parameter is not set. So, when the QueryChangedDiskAreas API is invoked, it returns an error. For more information, refer to http://kb.vmware.com/kb/1033816. To correct this problem, ensure that no snapshots exist on the virtual machine before selecting the **Enable Changed Block Tracking for VM** check box for the initial backup.

Description	Symptom	Solution
Incremental or Differential Image-Level Backup fails for a restored virtual machine.	After restoring a virtual machine, when you perform an Incremental or a Differential Backup, the job fails with the following error message in the NVBU Logs: **"Failed to get changed disk areas."**	After restoring a CBT-based backup, you must start the backup sequence again with a new baseline Full Backup. The previous backup sequence of Incremental or Differential Backups (performed before the virtual machine was restored) gets invalidated at the time of restore and cannot be continued as such.
The File-Level Backup Method does not back up data through a reparse point.	When a disk that is mounted as a reparse point on a Guest OS is included in a file-level backup, the backup completes without any errors or warnings. However, the Plug-in *for VMware* does not actually back up any data for a reparse point. It is listed as an empty node in the **NVBU Restore** window.	Currently, the VMware API does not support this type of backup. Workaround: ■ Install an NVBU Client on the Guest OS, and perform a backup using the Plug-in *for FileSystem* to include the reparse point directory. – or – ■ Mount the disk as drive letter instead of a reparse point. Then, create a backup job to include the new drive letter.

Restore job fails.	A restore job fails with the following error:
	Log Message: **"Failed to restore VM disk data."**
	Log Context:
	`Failed to open vmdk`
	`VDDK error encountered: code 13`
	`Retrieving error message text`
	`VDDK error message is 'You do not have access rights to this file'`
	`Disk data restore failed for '[datastore]VirtualMachineName/VitrualDiskName.vmdk'`
		The NVBU Client running the Plug-in *for VMware* may not have access to the SAN. To verify, try using the NBD Transport Mode. If the restore completes successfully with this mode, it indicates SAN connectivity issues.
		To use the SAN transport mode, the Plug-in *for VMware* host must have SAN connectivity to the VMFS LUN. Ensure that the LUN is accessible and the SAN is configured correctly.

Description	Symptom	Solution

Restore job fails.	A restore job fails with the following error:
	Log Message: **"Failed to add VM to target server's inventory."**
	Log Context:
	`"Fault string is 'Invalid configuration for device '3'.'"`
	When this error occurs, enable trace and run the restore job again. When the job completes, open the **vmw<nnn>_soaprecv.log** file, and check if it contains an XML **<WaitForUpdatesExResponse>** message with contents similar to the following:
	`<val xsi:type="LocalizedMethodFault"> <fault xsi:type="InvalidDeviceSpec">`
	`<property>deviceChange[3].device.backing.fileName</property>`
	`<deviceIndex>3</deviceIndex>`
	`</fault>`
	`<localizedMessage>Invalid configuration for device '3'.</localizedMessage> </val>`
	If yes, it indicates that the backup contains an invalid configuration for a CD or DVD drive.
		To correct this problem, use the following steps:
		1. Open the **vmware.cfg** file in a text editor. This file is located in the **<NVBU Installation Directory>/config/** directory.
		2. Edit the following entry, and set it to **"True"**:
		`[Custom:ReconfigureVirtualCdromDevices] Value=True`
		(By default, this parameter is set to **"False"**.)
		3. Rerun the restore job. It will complete successfully. If a CD or DVD drive was set to **"Host Device"** or **"Datastore ISO File"** type during the original backup, it will be reconfigured as **"Client Device"** type. A warning message in the logs will provide a list of reconfigured devices. The log context will include their original configuration. To view the log context, double-click the log message.
		4. After restoring the virtual machine, reset the **[Custom:ReconfigureVirtualCdromDevices]** parameter to **"False"**.

9.2.0 SOAP Messages

When tracing is enabled, the Plug-in *for VMware* generates the following two files along with the other NVBU trace files:

- **vmw(nnn)_soapsent.log**
- **vmw(nnn)_soaprecv.log**

These files contain the communication details between the Plug-in *for VMware* and the vSphere web service running on the VMware vCenter or ESX/ESXi Servers.

When you send the trace files to Quest Customer Support, ensure that these two files are also included.

9.3.0 VDDK Logs

The Plug-in *for VMware* uses the VMware VDDK API for image-level backups and restores and file-level browse and backup operations. To diagnose or troubleshoot errors encountered during such operations, Quest Customer Support may request for VDDK logs. For generating these logs, follow these steps:

1. Open the **vmware.cfg** file in any text editor. This file is located in the **<NVBU Installation Directory>/config** directory.
2. In the **[Custom:GenerateVddkLogsOnDisk]** section, set the **Value** parameter to **True**:

   ```
   [Custom:GenerateVddkLogsOnDisk]
   Value = True
   ```

Important: By default, this value is set to **False**, and must be left so unless requested by Quest Customer Support.

3. Retry the operation with the new setting. This will generate VDDK logs entitled **vixDiskLib*.log** in the following directories:
   - **Windows**

     `<SYSTEMDRIVE>\WINDOWS\Temp\vmware-SYSTEM`
   - **Linux**

     `/tmp/vmware-root`
4. After capturing the logs, reset the value to **False**.